

HOTPin

Installation Guide

Celestix HOTPin Appliance

celestixThe logo for Celestix, featuring the word "celestix" in a white, lowercase, sans-serif font, followed by a red stylized arrow pointing upwards and to the right.

Celestix HOTPin Installation Guide
Document Number: HPN0030-946-003
Part Number: (CCD) 1005-00000015

Updated: June 28, 2013

Celestix HOTPin 2FA system software version 3.7

© 2013 Celestix Networks, Inc. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

HOTPin, Celestix and Celestix logo are registered trademarks or trademarks of Celestix Networks, Inc.

Microsoft, Microsoft logo, Microsoft Windows Server, Microsoft Forefront, Threat Management Gateway, Unified Access Gateway, Active Directory, Windows, Windows NT, ActiveX, Internet Explorer, Windows Phone, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mac, iOS, iPhone, iPod touch, iPad and Safari are either registered trademarks or trademarks of Apple Inc., registered in the U.S. and other countries.

Google Play is a registered trademark of Google, Inc. in the United States and/or other countries. Android is a trademark of Google Inc.

The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Celestix Networks is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.

Juniper Networks is a registered trademark of Juniper Networks, Inc. in the United States and other countries.

Oracle and JavaScript are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
Installation Guide Usage Notes.....	1
Verify Package Contents.....	4
Appliance Hardware Features	5
HOTPIn System Overview.....	6
The Next Step	10
Install the Appliance	12
Installation Assumptions	12
Network Information Worksheet	13
Rack Your Appliance	14
Connect Your Appliance to the Network	15
Front Panel Controls Overview	17
Power Your Celestix Appliance	17
The Next Step	18
Configure the HOTPin System	19
Configure the Appliance	19
Configure the Application	27
The Next Step	59
HOTPIn User Accounts	60
Manage User Accounts.....	61
Client Software	75
Download User Token Key.....	76
The Next Step	79
Create a System Image.....	80
System Image.....	80
LGV.....	82
Update Software	83
Appendices.....	84
HOTPIn Glossary.....	85
Web User Interface Content Overview	92
Additional Features	93
API Extensions	94
Safety Precautions	95
Product Reclamation and Recycling	96
Network Information Worksheet Form	97

Introduction

Celestix Networks delivers an exceptional combination of perimeter security features, scalability, and simplicity in cost-efficient appliances. Ready-to-deploy appliances offer decreased complexity and easier management that reduce the risk and cost of security solutions. The Celestix line of appliances provides key security framework components: firewall, branch-office connectivity, web cache/proxy, wireless policies/authentication, remote access (SSL and traditional VPN), two-factor authentication, patch management, anti-spam/anti-virus gateway deployments, and data management/protection. Celestix appliances provide the best option for today's demanding IT infrastructure security needs.

The foundation of your appliance is the Comet engine running on Windows Server® 2008 R2 Embedded. Comet provides convenient access to administration functions like setup, network configuration, and server task management through a web user interface. The web user interface is referred to as the web UI in both print and online documentation.

HOTPin™ appliances provide cost efficient, customizable two-factor authentication (2FA) for access to your organization's network resources. HOTPin is grounded in the HMAC-Based One-Time Password Algorithm ([RFC 4226](#)). The system's two factors are a user-defined personal identification number (PIN) and a one-time password (OTP). OTPs are codes that are generated from token keys. Keys are created for individual users. Users authenticate by entering their user name, PIN and an OTP at login.

HOTPin can also be configured for one-factor authentication (1FA) by disabling the PIN feature. This may be appropriate for organizations that employ other authentication methods, like Active Directory®. HOTPin then provides one authentication factor (the OTP), and the other method provides the second (a password, for example). Administrators should note that disabling the PIN feature without combining another authentication form with HOTPin (as mentioned above) would not be secure.

The 3.7 update to the HOTPin system adds the following functionality:

- NPS RADIUS client import/export
- QR Code authentication
- API SDK
- HOTPin Agent 1.1 update

NPS RADIUS client configurations can now be transferred to and from HOTPin server for backup or batch configuration. QR code authentication offers simplicity and security because scanning a code is easier and reduces exposure when using public, untrusted computers to access resources. The API SDK allows organizations to customize authentication communication. HOTPin Agent provides API extensions to allow authentication from any website login page.

Installation Guide Usage Notes

This guide is intended to help system administrators install and configure a new appliance with a base level setup as quickly as possible. The instructions cover steps for common deployment scenarios. They usually offer one option to accomplish a task, though there may be other ways to achieve the same thing. The guide does not provide extensive reference information. Online help in the web UI can provide additional information.

Document conventions:

- Using a PDF viewer besides Adobe® Reader® may disable some of this document's functionality and may change how the content displays.
- Instructions are generally intended for administrators to manage the appliance installation through Comet's web user interface administration tool.
- The appliance administration website, or web user interface, is referred to as the web UI.
- Access to the web UI is assumed to be through Internet Explorer® (IE). You can use another browser, however some functionality requires IE.
- Instructions are presented in the order you should follow to set up your appliance.
- Web UI on-screen items are noted in **bolded type** for easy identification.
- Features on the appliance front and rear panels are also noted in **bolded type**.
- When referring to subsections in this document, the hierarchy is delineated by a colon.

*For example, the location of the section *To enable the alert email feature* would be delineated as Quick Setup Steps : Alert Email : To enable the alert email feature.*
- Instructions assume the reader will navigate from the web UI main menu bar.

For example, to access appliance static routes, hover over the **Network** option on the main menu bar, scroll to and hover over **Routing**, then scroll to and click **Static Routes**. The navigation path will be delineated as **Network|Routing|Static Routes**.

- While network interface connections are commonly referred to as NICs, ports and adapters, the document uses network adapters as a simplified reference.
- When discussing your HOTPin appliance, the document generally refers to the *appliance*.

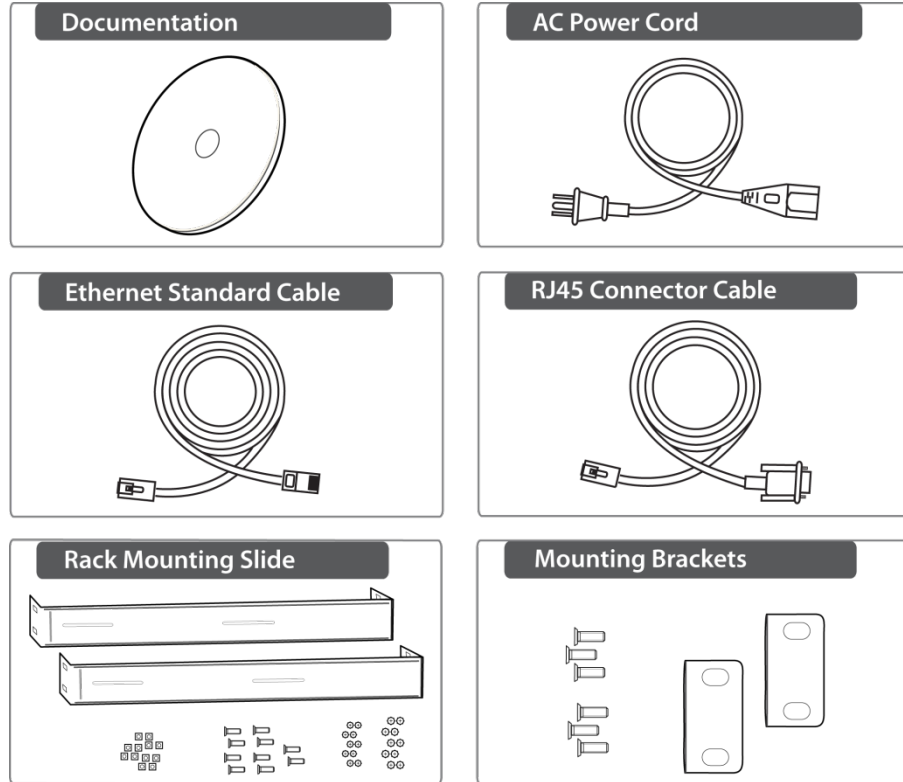
Web User Interface



The web UI is a management tool to access the most common features of your Celestix appliance. Initially, you will use it to quickly set up your appliance. Subsequently, you can use the web UI to access administrative features for both Comet and the HOTPin application.

See the Appendix topic [Web User Interface Content Overview](#) for features included in the web UI. See the online help topic **Web User Interface Overview** for more information about using the web UI (**Help|Contents|Web UI Overview**).

Verify Package Contents

The following identifies standard package items that may be included with your appliance. See the list below it for the items included with each appliance series.



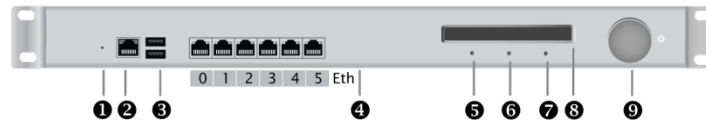
Appliance Series	3200	6200
Contents		
Documentation CD	✓	✓
CAT6 Ethernet Cable	✓	✓
Power Cable	✓	2
RJ45 Connector Cable	✓	✓
Mounting Brackets & Hardware	✓	x
Rack Mounting Slides & Hardware	x	✓
✓ - included x - not included		

If an item is missing from the package, contact Celestix Networks via e-mail:

Support@celestix.com

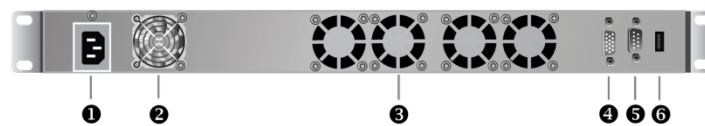
Appliance Hardware Features

1500/3200/4200 series | Front View



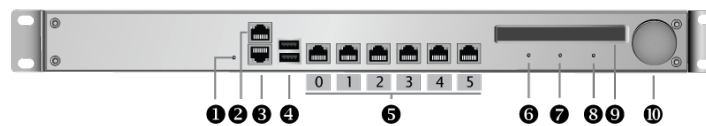
- ❶ Reset
- ❷ RJ45 Connector
- ❸ USB Ports
- ❹ Gigabit Ethernet Ports
- ❺ Alert Indicator
- ❻ Hard Drive Status Indicator
- ❼ Power Status Indicator
- ❽ Front Panel Display
- ❾ Jog Dial

1500/3200/4200 series | Rear View



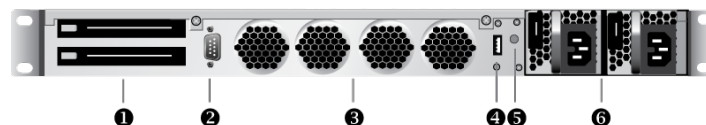
- ❶ Power Supply Inlet
- ❷ Power Supply Cooling Fan
- ❸ Cooling Fans
- ❹ VGA Port
- ❺ DB9 Com Port
- ❻ USB Port

6200 series | Front View



- ❶ Reset Button
- ❷ IPMI Port
- ❸ RJ45 Connector
- ❹ USB Ports
- ❺ Gigabit Ethernet Ports
- ❻ Alert Indicator
- ❼ Hard Drive Status Indicator
- ❽ Power Status Indicator
- ❾ Front Panel Display
- ❿ Jog Dial

6200 series | Front View



- ❶ Hot Swappable Hard Drives
- ❷ VGA Port
- ❸ Cooling Fans
- ❹ USB Port
- ❺ Alarm Reset Button
- ❻ Hot Swappable/Redundant Power Supply

Appliance Configurations

Your appliance is a member of a versatile series of security products. The following table will help you to identify your configuration information.

Appliance Models		
Model	Hardware Platform	Rack Size
3200	X4	1U
6200	P2	1U

Appliance Naming Conventions

Your appliance name indicates the main components included in its hardware/software configuration. For example, if you purchased a WSA 4200, the appliance configuration would include an X4 appliance with the Forefront Unified Access Gateway application.

Please Note: Celestix appliances are available in various configurations. Find the model number on the front panel display.

HOTPin System Overview

The HOTPin system provides secure two-factor authentication through a passcode. The passcodes are generally composed of user-created personal identification numbers (PINs) and one-time passwords (OTPs), unless HOTPin has been configured for one-factor authentication, which then requires only the OTP. OTPs are token codes made up of a six-digit number string. The OTP/token codes are generated either by client software running on a PC/Mac/mobile device, a hard token device, or through token providers on the server. Token providers send OTPs to users through such methods as email, web applications, or text messages.

The following diagram represents the login process with the possible OTP generation methods.

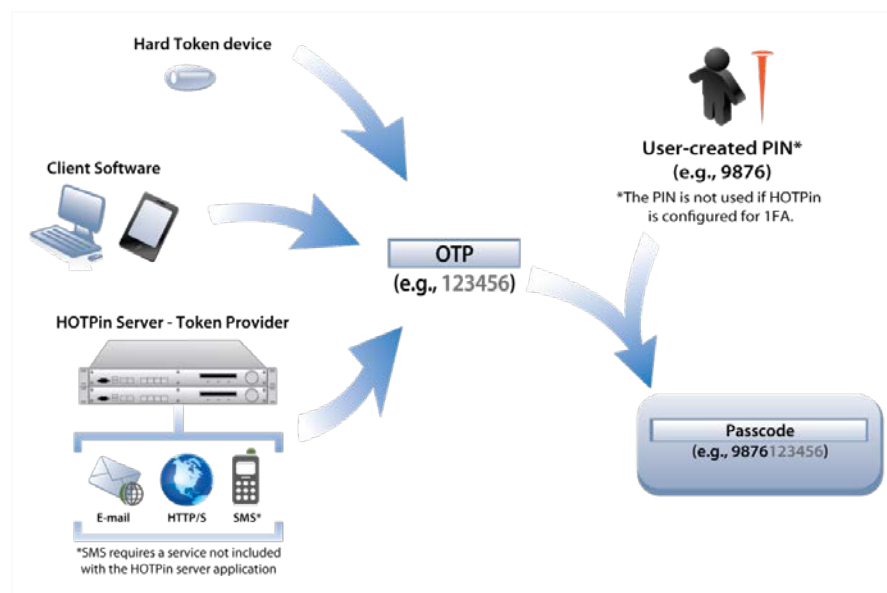


Illustration 1 - Token Generation Options

Please Note: In the HOTPin system, OTPs and token codes are synonymous.

This section provides a brief overview to help system administrators become familiar with the HOTPin system. It reviews authentication methods and summarizes the configuration for a standard deployment. It also provides information about how HOTPin works with Active Directory and notes for client software platforms that have special considerations.

User Authentication

HOTPin requires a user name and passcode for login. A passcode includes personal identification numbers (PINs) and one-time passwords (OTPs) for two-factor authentication. A passcode for single-factor authentication HOTPin deployments just includes an OTP. In the HOTPin system, OTPs are also referred to as token codes. Each user has a unique token key and an incrementing counter to create the token code. That allows more secure login to a network from a remote device (for example, PC or mobile phone) because the code changes each time.

In two-factor authentication, PINs can be created in three ways:

- Administrators can set the PIN through the web UI.
- User can set the PIN through the HOTPin User Website.
- Users can create a PIN the first time they log in.

Until the PIN is created, the user account is in New Pin Mode. Once a PIN is created, it will be used for each subsequent login.

Some organizations do not require that a PIN be included in the passcode because they also use another form of authentication at login (like Active Directory). While it may be sufficient to use HOTPin as single-factor authentication in specific cases, each organization should thoroughly evaluate the risks before choosing to disable the PIN requirement.

Token code generation methods are discussed in the following three topics.

Client Software Tokens

Software tokens, generally referred to as client software, are client software token applications that must be installed on PC's, Macs, or mobile devices to generate the token codes used in passcodes. The client software essentially turns a user device like an iPhone® into a token. Client software may also be referred to as a soft token.

Token Devices

A token device, also referred to as a hard token device or hard token, generates token codes using an external key that must be imported to HOTPin. Once the key has been imported, it can then be assigned to a user account. The key on the server must be in sync with the device to produce valid token codes for login. Key fobs are a common token device.

Token Providers

Token providers send the token codes used in passcodes to users from the server. The Email OTP Provider can send a token code to an email address or a mobile device that can receive text messages (requires phone service that provides an SMS gateway). The HTTP OTP Provider can use a web application or SMS server to send a token code to a mobile phone. The SMS OTP Provider can send codes through a modem attached to the HOTPin Server.

Please Note:

- › To maintain synchronization with the server, a user should use only one token code generation method at a time.
- › If using client software or a hard token, a user should only use one device at a time.

User Login Information

You will need to provide your end users with information for setup and login. The HOTPin system includes a User Login Information Sheet to help you organize the information you need to provide. Go to **HOTPin|Documentation** to download the PDF form.

General Setup Information

The following outlines the general steps for setup. It is intended to provide a high level view and includes branches for token generation options.

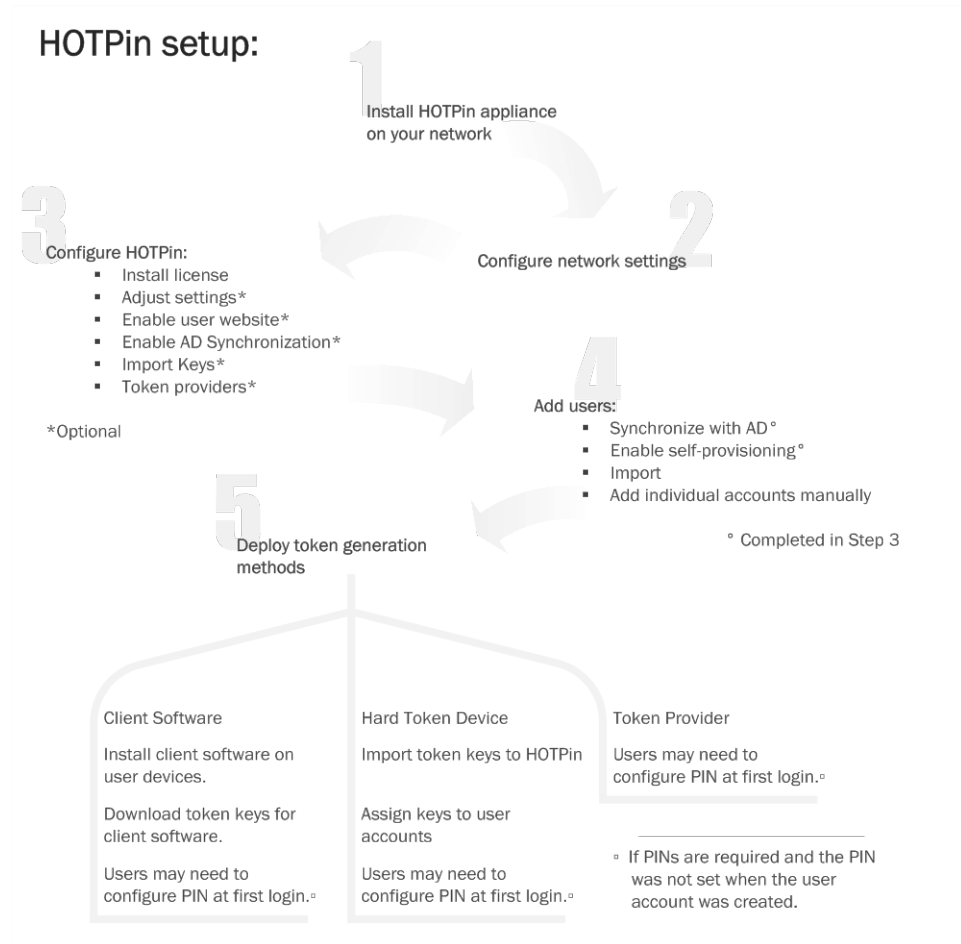


Illustration 2 – General Setup Overview

End users can complete steps 4-5 without administrator assistance if the **HOTPin User Website** is enabled for self-provisioning.

Version Information

The HOTPin application version is noted in the title on the main help page; see **Help|Contents|HOTPin**.

Active Directory

The HOTPin system works in concert with Active Directory (AD) in several ways:

- User management
 - ♦ User account maintenance
 - ♦ User self-provisioning

- ♦ Import
 - Token key download through client software
 - Single sign-on

User management includes the [AD Synchronization](#) and [HOTPIn User Website](#) features, in addition to the ability to manually [import](#) accounts from AD. Token key download is the client software Import from Network feature that enables users to get token keys through the LAN. And HOTPin can be combined with AD to allow single sign-on to your network.

If you use AD Synchronization, the HOTPin User Website, or import users from AD manually through the web UI, then HOTPin user names will likely match an AD property (for example, SAM account name, UPN, or email address); once a property has been selected, the same property should be used for all accounts. If different properties are assigned to accounts, users may experience trouble authenticating or getting keys. If you don't enable syncing or the user site, but want single sign-on functionality, you will need to make sure that HOTPin user names match the AD authentication property.

Client Software Notes

Windows PC and Mac clients are available for download from the web UI and HOTPin User Website. Other clients are available from the download site for the device platform. The applications are free, but usually require an account for the site to download.

iOS Considerations

- iOS clients version 2.0 and earlier can only import a token key from the network. The file import or data string features are not supported. This means that System Administrators must enable the HOTPin User Website to support the earlier client application versions.
- iOS client version 3.0 can import keys from the network or add them from data strings. The feature to import from file is not supported.

The Next Step

The following sections guide you through HOTPin setup. First you will install the HOTPin appliance on your network, then you will configure application settings. Depending on your application setup choices, you may need to add user

accounts to HOTPin (if not [syncing with AD](#) or enabling the [HOTPin User Website](#) to allow self-provisioning); instructions are in the [HOTPin User Accounts](#) section.

Install the Appliance

The guide provides a system administrator with concise instructions for a base deployment. The document covers common installation requirements and is not intended to be comprehensive. Every network environment is different, and some installations may require additional configuration.

Installation instructions first cover assumptions the guide takes into account for a common deployment to help administrators plan for the skills and resources they may need. Assumptions are followed by the network information worksheet. The worksheet helps to gather necessary information that will aid in the installation process. Preparation steps are followed by instructions to rack, connect to the network, and power the appliance.

Installation Assumptions

The following sections provide information about necessary skills/knowledge administrators should have and the assumptions that cover appliance installation for a majority of network settings.

Skills and Knowledge

System administrators should be familiar with:

- Windows server management
- Microsoft's Active Directory
- Networking technology

Network Settings

The following general conditions apply to the instructions contained in this guide. Again, your network settings may differ and could require some adjustment to the general information presented herein.

- Your LAN is configured for DHCP. You will use DHCP initially to assign an IP address to the LAN0 network adapter. You can find the assigned IP address on the front panel display.
- Instructions generally refer to Active Directory (AD) as an example domain controller.
- Instructions to access the web user interface (web UI) cover a client computer running Internet Explorer® 7.0 or higher.

Note: IE running on a Windows® computer is required to access the web UI's full functionality.

- You have static IP addresses reserved for network adapters as needed.

Network Information Worksheet

It will be helpful if you gather and verify your network information before you begin appliance installation and setup. By filling out the Network Planning worksheet, you can expedite your installation. An example of the worksheet is provided below with descriptions for the information it includes. A blank copy of the worksheet is included in the Appendix for your use.

Please Note: Incorrect network configuration could compromise or impede the HOTPin appliance.

Network Information Worksheet (example)		
Property	Network Information (example)	Explanation
Computer Name		The appliance must be assigned a computer name. The computer name must be 15 alphanumeric characters or less. This information is needed in: Quick Setup : Server Name
Administrator Password	[Celest1x] (default)	The administrator password is the password used to log on to the appliance. Define the administrator password during setup using at least six characters and at least three of these four categories: <ul style="list-style-type: none"> ▪ Uppercase letters ▪ Lowercase letters ▪ Number ▪ Non-alphanumeric characters (for example, !, \$, #, %) <p>Note: The default user name is “administrator” and the default password is “[Celest1x]” (case sensitive, brackets included). The system administrator should change the default password in the Quick Setup steps.</p> <p>This information is needed in: Quick Setup : Administrator Password</p>
Workgroup or Domain name		Record the name of the Workgroup or Domain that will be joined during setup. This information is needed in: Quick Setup : Server Membership
Network Adapters	IP Address: Subnet Mask: Default Gateway: Primary/Secondary DNS Server(s): Static Routes: Network Address: Gateway Address:	This information is needed in: Quick Setup : Interfaces
Active Directory Server	IP Address: Hostname:	This information may be needed for application setup.
Application Server	IP Address: Hostname:	This information may be needed for application setup.

Illustration 3 - Network Planning Form Example

Rack Your Appliance

Your Celestix appliance is a 1U or 2U device that should be attached to a standard 19-inch equipment rack as follows:

Note: If your appliance shipped with slides instead of brackets, see the instructions included in the slide packaging for the rack mounting procedure.

1. Select a secure location where only authorized personnel can access the appliance.
2. Mount the appliance on your rack:
 - a. Use all the provided screws to attach mounting hardware to the front right and left of the appliance.
 - b. Attach the appliance to the front supports of your equipment rack using a screw (not provided) for each of the holes on each of the brackets. For example:



Caution:

- ✓ Do not place the appliance on the floor.
- ✓ Keep it in an upright position.
- ✓ Place it in a well-ventilated area that is out of direct sunlight.

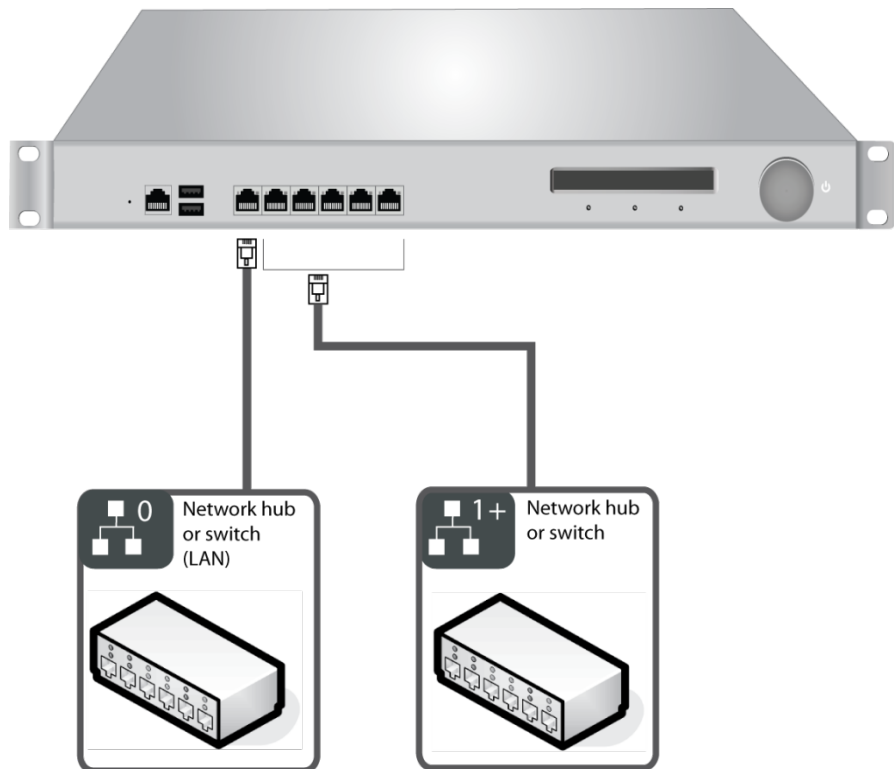
Connect Your Appliance to the Network

As mentioned previously, these instructions assume that your network is configured for DHCP. You will initially obtain an IP address through DHCP; configuration for a static address is covered during set up (in the [Interfaces](#) section).

To connect your appliance:

1. Connect an Ethernet cable from the LAN0 adapter on the Celestix appliance to your internal network hub or switch.
2. **[Optional]** For additional network connections, use the LAN1 network adapter (or above) on the appliance

The diagram below provides a reference.



Please Note: Your appliance hardware may look somewhat different from the example. Most deployments will, however, connect to the network in a similar fashion.

Network Interface LED indicators:

Each of the network adaptors contains a pair of lights to help identify connection speed and usage. See below for details (listed by model number):

- 1500/3200/4200/5200
 - ♦ Right light – displays connection speed (unlit 10Mbps, green 100 Mbps, orange 1000 Mbps).
 - ♦ Left light – displays activity (blinking indicates traffic, unlit indicates no traffic).
- 6200
 - ♦ Right light – displays connection.
 - ♦ Left light – displays activity (blinking indicates traffic, unlit indicates no traffic).

Front Panel Controls Overview

The front panel contains an LED display and jog dial. These controls allow you to view system information and to directly manage some configuration settings on the appliance. You will use these controls to complete your appliance configuration.

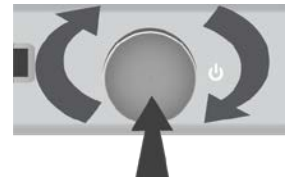
Front Panel Display

The front panel display operates in two modes:

- Idle mode – the default mode; status screens cycle through display.
- Configuration mode – press the Jog Dial to enter configuration mode; see the [Jog Dial Operation](#) section below for more information.

Jog Dial Operation

The Jog Dial on the appliance front panel is used to navigate the LED display.



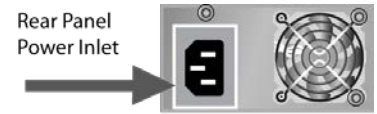
- Turn to scroll through screen options.
 - ♦ The square brackets cursor [] allows you to scroll through items on the screen when the front panel display is in configuration mode. The following example shows the Add option selected by the cursor:
[Add]
 - ♦ The angle brackets cursor > < allows you to edit options after selection when the front panel display is in configuration mode. The following example shows the Delete option selected by the cursor:
Add
> Delete <
- Press to select options.

Power Your Celestix Appliance

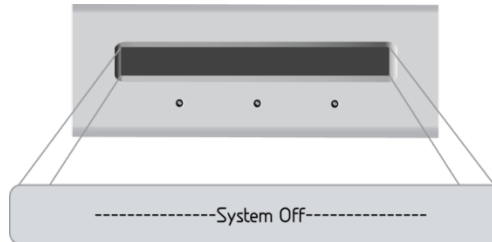
The following instructions guide you through connecting power and turning on your appliance.

To connect your appliance to a power source:

1. Connect the power cable from your power source (typically a UPS) to the power inlet on the rear panel. The power cable is included in the appliance packaging.

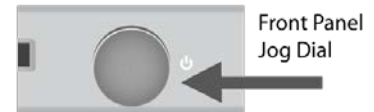


2. The display will show the **System Off** message:



Power On/Off Your Appliance

Power on and boot the appliance by pressing the Jog Dial.



It is possible to power off your appliance by pressing the Jog Dial for 5 seconds. However, you should use the Shutdown option from the front panel display menu to power off the appliance gracefully

The Next Step

Now that you have installed the appliance on your network you are ready to setup network information and the HOTPin application.

Configure the HOTPin System

This section provides instructions for the appliance setup and configuration that is required for all deployments. The first topic walks you through general network configuration for the appliance. The second topic guides you through both required and optional HOTPin application configuration.

Topics for each section include:

- Configure the Appliance
 - ♦ Configure Initial Access
 - ♦ Access the Web User Interface
 - ♦ Quick Setup Steps
 - Interfaces
 - Date/Time
 - Administrator Password
 - Server Name
 - Server Membership
 - Alert Email
 - Quick Setup Finish
- Configure the Application
 - ♦ Install Your License
 - ♦ Configure System Settings
 - ♦ Enable the User Website
 - ♦ Configure AD Synchronization
 - ♦ Import External Token Keys
 - ♦ Configure Token Providers

Configure the Appliance

The appliance configuration instructions guide you through general server and network configuration. For example, you will configure IP address information, set the server name, and can also set up alert email.

Configure Initial Access

The appliance can be deployed in a network that does not use DHCP, but it is generally easier to start setup with a DHCP-assigned IP address for your internal network (LAN0) adapter. If you need to assign IP addresses to any adapters manually, you will use the Jog Dial/front panel as explained in the next section, [Configure IP Address without DHCP](#).

Configure IP Address without DHCP

Skip this section if your network uses DHCP. Instead, start with the section [Access the Web User Interface](#).

You will need the IP address for your internal network (LAN) adapter to access the appliance administration website, or web UI, which you will use to complete the setup for your appliance. If you can't use DHCP, this topic explains how to do it manually through front panel controls. If you enter the internal network adapter (LAN) IP address through the front panel, you will not need to do it in the later section, Quick Setup Steps : [Interfaces](#).

To change the internal network IP address:

Note: You will only need to follow this step if you do not have DHCP configured for your network.

1. Press the Jog Dial and scroll to > **Configure Network** <.
2. Press the Jog Dial again to select.
3. If necessary, press the Jog Dial and scroll to and select **LAN**. The display should show [**LAN0**].
4. Scroll to and select [**Next**] to continue.
5. Scroll to and select [**Static IP**].
6. Enter the IP address:
 - a. Press the Jog Dial to edit the first octet of the IP address.
 - b. Turn the dial to change the number.
 - c. Press the Jog Dial again to complete entry.
 - d. Repeat for the remaining octets.
7. Scroll to and select [**Next**] to continue.
8. Enter a Netmask if needed.
9. Scroll to and select [**Proceed to Configure**] to save your entry. You will see the **Configure Network** screen when the process has completed.
10. Scroll to > **Back** < and select to return the front panel display to idle mode.

If you need to configure other adapters, you can repeat the instructions above as necessary, or you can follow the steps in the Quick Setup Steps : [Interfaces](#) section.

Access the Web User Interface

You are now ready to configure your appliance using the web UI. If the LAN IP address was assigned through DHCP, use the Jog Dial on the appliance front panel to scroll to LAN and note the assigned IP address.

From a client computer on your network, default access to the appliance web UI is through Internet Explorer at [https://ServerName|IP address:8098](https://ServerName/IP address:8098).

For example, if your server IP address is 192.168.30.4, the web UI URL would be <https://192.168.30.4:8098>

Important: You may see a certificate warning when you access the site because it uses a self-signed certificate. You will need to accept the certificate to access your appliance.

You will be prompted to enter your administrative credentials. Before going through the Quick Setup process, the credentials to login are:

User name: administrator

Password: [Celest1x]

Please Note:

- The password is case-sensitive and the brackets are included.
- You may be required to enter the user name in the “domain\administrator” format.
- Internet Explorer is required for full functionality in the web UI.

After successful login you will see the Start web UI screen:

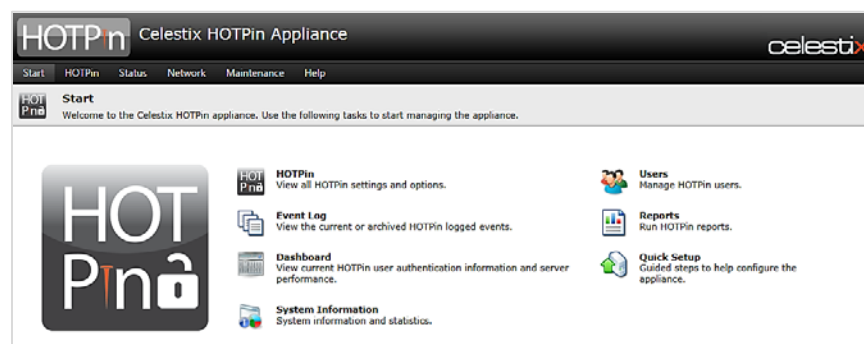


Illustration 4 - Start Screen

The main HOTPin screen is accessed when you click the **HOTPin** in the menu bar:

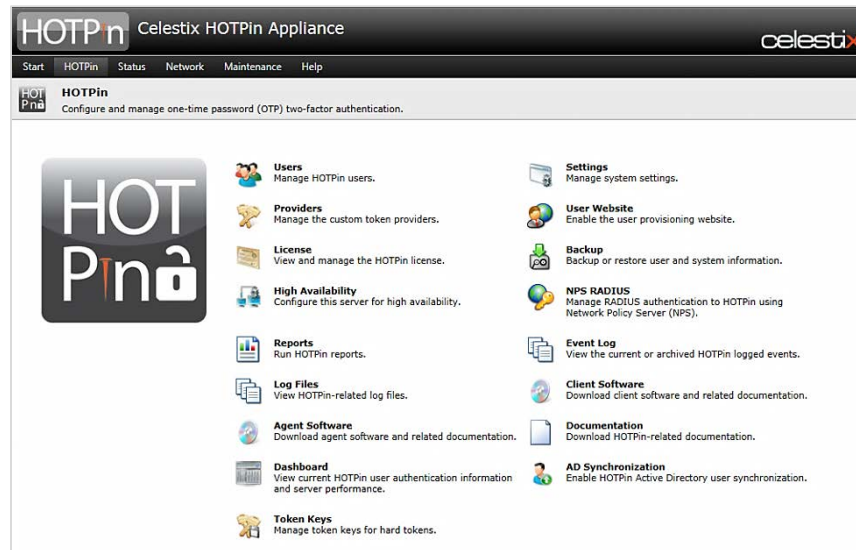


Illustration 5 - HOTPin Main Screen

Quick Setup Steps

The following sections provide instructions for basic appliance configuration. They are presented in the order in which you should complete them. You can access **Quick Setup** through the **Start** menu in the web UI.

Interfaces

The Interfaces function provides access to appliance network adapter configuration. A network adapter is used for Ethernet connections and is both the physical interface, or connector, and the hardware for access to a network. An adapter is also commonly referred to as an adapter card or a network interface card (NIC). This section provides a brief description of the configuration settings in the Interfaces web UI feature and how to access them.

Use the **Interfaces** function to assign either DHCP or static IP addresses to network adapters.

The list of interfaces includes the following information:

- **Name** – displays Ethernet connection identification.
- **Device Name** – displays hardware adapter identification.
- **IP Address** – displays the Internet Protocol address.
- **Configuration** – indicates either a **DHCP** or **Static** IP address.

- **Status** – indicates **Up** for adapters with connected cables; indicates **Down** for either an unused adapter or a connection issue.

General Properties

Select a connector to enable the **General Properties** button. Use this function to assign DHCP or static address configurations. A static address includes these settings:

- Internet Protocol (IP) address
- Subnet mask
- Gateway address

You can also specify automatic or preferred DNS server settings on this screen.

To access network connection configuration:

1. Navigate to **Network|Interfaces**.
2. Select an adapter.
3. Click **General Properties**.
4. When you are done entering information, click the **OK** button to save your settings.

Important: An interface, or adapter, must be connected before it can be configured. A warning will be displayed if you attempt to configure an unconnected adapter.

Date/Time

This section provides a brief description of the configuration settings in the date and time web UI feature and how to access them.

To access date and time configuration:

1. Navigate to **Maintenance|Date/Time**.
2. See the settings description below for information.
3. Click the **OK** button to save your settings.

Date and Time Settings Include:

- **Date:** format mm/dd/yyyy.
- **Time:** format hh:mm:ss am/pm.

- **Time zone:** select a city that represents your time zone from the drop menu.
- **Automatically adjust clock for daylight savings:** select to instruct the server to change time according to daylight saving/standard time.

Administrator Password

Your appliance ships with a default administrator password. You should change the password when you set up your appliance as this password is public knowledge. This section provides a brief description of the configuration settings in the Administrator Password web UI feature and how to access them.

Please Note:

- The Administrator password feature only allows you to change the administrator account password; it does not provide access to change passwords for members of the local Administrators group.
- Domain users are not allowed to change the administrator account password. You must be logged in using the administrator account to change its password.

To change the administrator account password:

1. Navigate to **Start|Quick Setup|Administrator Password**.
2. When the **Administrator Password** screen opens, you will see the following fields to edit:
 - **User Name** – the administrator user account name is displayed.
 - **New password** – enter a new password.
 - **Confirm password** – confirm the new password.

Note: Password complexity requirements are noted on the **Administrator Password** screen.
3. Click **OK** when you have completed the updating the password.

An error message will inform if the change was not successful.

Server Name

Server names are used to help identify your appliance on the network and to facilitate client access. This section provides a brief description of the configuration settings in the Server Name web UI feature and how to access them.

To add or change server or domain settings:

Important: You will need to reboot the server to complete these steps.

1. Navigate to **Network|Server Name**.
2. Enter information for the following fields:
 - **Server Name** – specify a name for your appliance.
 - **DNS suffix** – optional; this field sets the primary DNS suffix. Specify the DNS suffix to create a fully qualified server name.
 - **Change primary DNS suffix when domain membership changes** – check this box if you want to update the primary DNS suffix when the appliance domain membership is changed (for example, at **Network|Server Membership**).
3. Click the **OK** button to save your settings.

The web UI will refresh and open to the **Quick Setup** screen after the appliance has finished the configuration change. Changing the Server Name may cause Internet Explorer to prompt you to accept the server certificate again.

Server Membership

Server Membership indicates the type of network to which your appliance is connected. This section provides a brief description of the configuration settings in the Server Name web UI feature and how to access them.

While domain membership is optional, your appliance needs to belong to some type of network group, like a workgroup or Microsoft Active Directory.

If you use Active Directory on your network, you will select the **Domain** option and specify the name associated with it.

If your deployment does not require joining a domain, select the **Workgroup** option and provide a name to identify it in the accompanying text field. Workgroup is the default setting.

To join the appliance to a domain:

Notes:

- › These instructions require credentials for a user with permission to add a computer to the domain.
- › You will need to reboot the server to complete these steps.

1. Navigate to **Network|Server Membership**.
2. Select the **Domain** option and enter your network domain name in the text field.

3. Enter a **User name** and **Password** in the text fields provided.
4. Click **OK**.
5. You will be prompted to reboot your appliance to complete the above changes:
 - Click **OK** to proceed with restarting your appliance.
 - Click **Cancel** to skip restarting your appliance. (You will need to restart the appliance later to complete the membership changes to **Network|Server Membership**.)

The web UI will refresh and open to the **Quick Setup** screen after the appliance has finished the configuration change.

Alert Email

Use the Alert Email function to allow/disallow your appliance to send system alert messages through a network SMTP server to addresses you specify. SMTP is required to use the Alert Email function. This section provides a brief description of the configuration settings in the Alert Email web UI feature and how to access them.

Please Note: Alert email is an optional configuration.

Use the following information to configure alert email:

- **Send error alert email** – select to enable your appliance to send alert types where the level is set to Error.
- **Send warning alert email** – select to enable your appliance to send alert types where the level is set to Warning.
- **Send informational alert email** – select to enable your appliance to send alert types where the level is set to Information.
- **To** – indicate one or multiple recipients. For multiple addresses, use a comma to separate each address.
- **From** – indicate an address that the recipient will recognize.
- **With** – enter your network SMTP server name or IP address.
- **Test Settings** – click this screen button to send a test email using the settings you entered.

To enable the alert email feature:

1. Navigate to **Maintenance|Alerting|Alert Email**.
2. Select **Enable alert email**.
3. Select the check boxes for the alert levels (error, warning, critical) you want email to be sent.
4. Enter a recipient address in the **To** field.

5. Enter a send address in the **From** field.
6. Enter your network's SMTP gateway name or IP address in the **With** field.
7. To test the email delivery, click **Test Settings**.

Note: The alert email function will indicate whether a test email was sent. If the test email is not received after the alert email feature indicates that one was sent, the error is most likely due to SMTP server settings. An error will occur if the SMTP service is not running or if your appliance is not correctly configured to see the SMTP server. Confirm your SMTP server and network settings before trying to test again.

8. Click **OK** to complete.

To disable the alert email feature:

1. Navigate to **Maintenance|Alerting|Alert Email**.
2. Select **Disable alert email**.
3. Click **OK** to complete.

Quick Setup Finish

The finish screen provides any final instructions or information if necessary for your installation. In addition, it provides a link to register your product with Celestix. Access the finish screen through the web UI at **Start|Quick Setup|Quick Setup Finish**.

Now that you have completed the configuration for your appliance, you are ready to configure the HOTPin server application.

Configure the Application

This section explains the HOTPin server application setup on the appliance. You will need to complete some or all of the following items – see descriptions for information.

- **Install your HOTPin license** – required for all deployments.
- **Configure System Settings** – if you need to change default settings.
- **Enable the User Website** – if you want to allow users to set up their own accounts, client software, and/or download token keys. The website is required to support users with iPhone clients prior to version 3.0.

- **Configure AD Synchronization** – if you want to streamline user management by linking the HOTPin user database to designated Active Directory OUs and/or groups.
- **Import External Token Keys** – if you provide users with devices like hard tokens.
- **Configure Token Providers** – if you will allow users to authenticate without client software or hard token devices; necessary if you want use email or compatible services like SMS to deliver token codes.

If neither AD Synchronization nor the HOTPin User Website is enabled, you will need to **add users** manually or **import** them in batches from Active Directory or a text file.

Install Your License

For evaluation purposes, the HOTPin system comes with a license for a limited number of users. Organizations must purchase a license that will cover the entire number of HOTPin user accounts that will be created. The License screen provides both information about the user license installed on your appliance and access to the License Upload Wizard.

View the following information on the License screen:

- **Product** – specifies the Celestix product.
- **Issued to** – specifies the organization authorized to install the purchased license.
- **Issued contact** – specifies the purchaser's email address.
- **Issued date** – displays the date the license was provided to the purchaser.
- **Serial Number** – displays the license serial number.
- **Expire date** – displays the last day the license will be valid.
- **User limit** – specifies the number of user accounts the HOTPin system will allow.
 - Note:** Disabled HOTPin accounts do count toward the user license limit.
- **Current users** – displays the total number of HOTPin users.
- **Status** – indicates whether a license is **Valid** or **Invalid**.

Please Note: A HOTPin license could be invalidated if the license expires, the number of user accounts exceeds the licensed quantity, or if the license file is tampered with.

To upload and configure your HOTPin license:

1. Save the license file (**license.xml**) to your appliance.
Caution: Do not change the name of the file; files of a different name will cause an error during upload.
2. Navigate to **HOTPin|License**.
3. Under **Upload new license**, click the **Browse** button to navigate to the license file.
4. Click **OK** to install the license.
5. A message displays when the license import has successfully completed.
6. Click **Cancel** to return to the main HOTPin screen.
 - Only valid license files will be allowed to upload.
 - An invalid file will produce an error message on the License screen.
7. Click **OK** to return to the **HOTPin** screen.

Please Note: The license covers the total number of users. If you have a license for 500 users, and have 490 accounts, deleting 10 users would mean that you would then have 20 available accounts.

Configure System Settings

Use the Settings page in the web user interface to define general settings for Authentication, Token Provider and Client Software and Passcode PIN features, and to access settings for Event Log and backup management. These features are described in sections below. Some default settings may serve common deployments; others like the Token Provider's Send Command String or backup options, should be customized as needed for your deployment.

To access system settings:

1. Navigate to **HOTPin|Settings**.
2. View or edit system property settings. See the topics below for property information.
3. Click **OK** to save changes and return to the main **HOTPin** screen.

General Tab

The general system settings provide configuration options for user-related functionality.

Authentication

Note: For both Authentication items, a lower value offers higher security, a higher value offers more flexibility.

- **Maximum Authentication Failures** – determines the number of login failures before a user is locked out of the system (each successful authentication resets the authentication failure counter). Once locked out of the system, the user will need to be unlocked by a system administrator (**HOTPin|Users**).

Note: It will be helpful to your users if you consider how long it will take them to log in when you set the maximum authentication failure feature in HOTPin. This is also true for timeout settings if you combine HOTPin with other authentication options. While these values should only be set as long or high as is necessary, consider that shorter duration timeout values/fewer login attempts may lead to system lockouts on legitimate users, especially for the first-time login where users may require two token codes to complete the process.

- **OTP look ahead value** – creates a window of valid token codes that can be used for authentication.

Token Provider

- **Sent Code TTL** – determines how long a token code will be valid when sent by a custom provider.
- **Send command string** – requests a token code from the HOTPin server when entered in the login page password field. If a PIN is required, the user combines the PIN and send command string separated by a comma (PIN,send). The command string is not case sensitive. A maximum of 32 characters can be used. The default value is *send*.

Important: Changing the string to a customized value from the default is recommended.

- **Increment authentication failures when code is sent** – limits the number of times a user can be sent a token code before successful authentication must occur. When enabled, the user's login authentication failure counter is incremented each time a provider sends a token code; the user will be locked out of the system if they exceed the maximum limit as defined in the Settings : Authentication : **Maximum Authentication Failures** field. The counter is reset after successful authentication.
- **Send ahead the next OTP** – provides the next valid token to end users. The provider will send another token code when a user successfully authenticates. The advance code is held in case users can't receive

OTP messages the next time they need to authenticate. The send-ahead code will be valid for the duration of the **Sent code TTL**.

Client Software

- **Require key passphrase** – sets the system default requirement option (includes the HOTPin User Website). When checked, the **Require key passphrase** setting will force users to create a passphrase in the client software application when the token key is imported. A user will then be prompted for this passphrase each time they load the key in the client, including when they open the client application. Administrators can override the requirement when downloading a key through the Users screen (**HOTPin|Users|Download Key**).
- **Clear key file after import** – sets the system default requirement (includes the HOTPin User Website). When checked, the **Clear key file after import** setting forces client software to overwrite the downloaded key configuration file and will then delete the file (if possible) after the key has been imported to the client. This prevents the user from reimporting the key at a later date when it would be out of sync with the server application. Removing the download file also prevents a malicious program from accessing it.

Passcode PIN

PIN required with token code when authenticating – check to require a PIN for user login. Uncheck to allow users to log in without a PIN. Disabling the PIN requirement allows users to log in with only a token code and changes the level of security in the HOTPin system from two-factor authentication to one factor. Removing the PIN requirement will not delete any of the PIN information stored in HOTPin user accounts. This means that if you enable the PIN requirement at some later time, PINs will be enforced for accounts that have previously created them, and all other accounts will be required to create PINs at their next login.

Note: HOTPin documentation generally assumes the most common deployment of the HOTPin system, where the PIN requirement is enabled, and thus references to passcodes generally include both the PIN and token code (OTP). If you disable the PIN requirement, the passcode will solely consist of the token code and your deployment may vary from the references noted in documentation.

Event Log Tab

Event Log system settings provide options to automatically truncate log content. Trimming the log, to keep it from growing too large, helps to maintain better database functionality in the HOTPin system. The default settings will be appropriate for most environments; however, some deployments may require an adjustment.

- **Enable event log trimming** – select to delete Event Log items that do not fall with the specified save period.
Note: Trimmed events are removed from the HOTPin Server database, but are not deleted from the Windows event log.
- **Save the last** – specify the period for which event log items will be saved.
- **Archive trimmed events** – select to save log items as text files before they are deleted from the Event Log; archived events are saved in Log Files (**HOTPin|Log Files|Help|Current Page**).

Backup Tab

HOTPin backup system settings provide options for automatic backup. Settings are described below.

- **Enable automatic daily backup** – select to allow automatic backups based on the following settings.
 - ♦ Time of day
 - ♦ **Backups to save** – indicate the number of backups.
Note: Each backup copy you retain requires disk space; thus, depending on your HOTPin deployment, a high number of saved backups could use considerable space on the appliance hard drive.
 - ♦ At least one of the following items must be checked if you enable automatic backups.
 - **Backup database** – select to include user information, logged events, HOTPin system settings.
 - **Backup license** – select to include the HOTPin license (**HOTPin|License**).
 - **Backup token provider configuration** – select to include provider settings in the backup (**HOTPin|Providers**).
 - **Backup NPS RADIUS** – select to include RADIUS client settings (**HOTPin|NPS RADIUS|RADIUS Clients**).
- Important:** There are no default backup items; you must select the components you want to backup.

Please Note: High Availability settings are not included in backup information. See online help for High Availability (**HOTPin|High Availability|Help|Current Page**) for information.

Enable the User Website

The HOTPin User Website is an appliance-hosted site on the local area network that can allow authenticated users to provision HOTPin accounts, client software, token keys, and instructions. You can enable or disable user self-provisioning on the User Website screen.

User Website Features

The user site configuration offers administrators discrete control over features like site login, creating/editing accounts, obtaining key configuration, and downloading client software/documentation. Disabling the site or individual features requires HOTPin administrators to perform more tasks to set up user accounts. The following diagram provides a reference.

Important: The diagram assumes that AD Synchronization has not been deployed. If you will deploy both the user website and AD Synchronization, you should consult the [AD Synchronization Compatibility](#) topic below for more information. User site functionality is affected by synchronization.

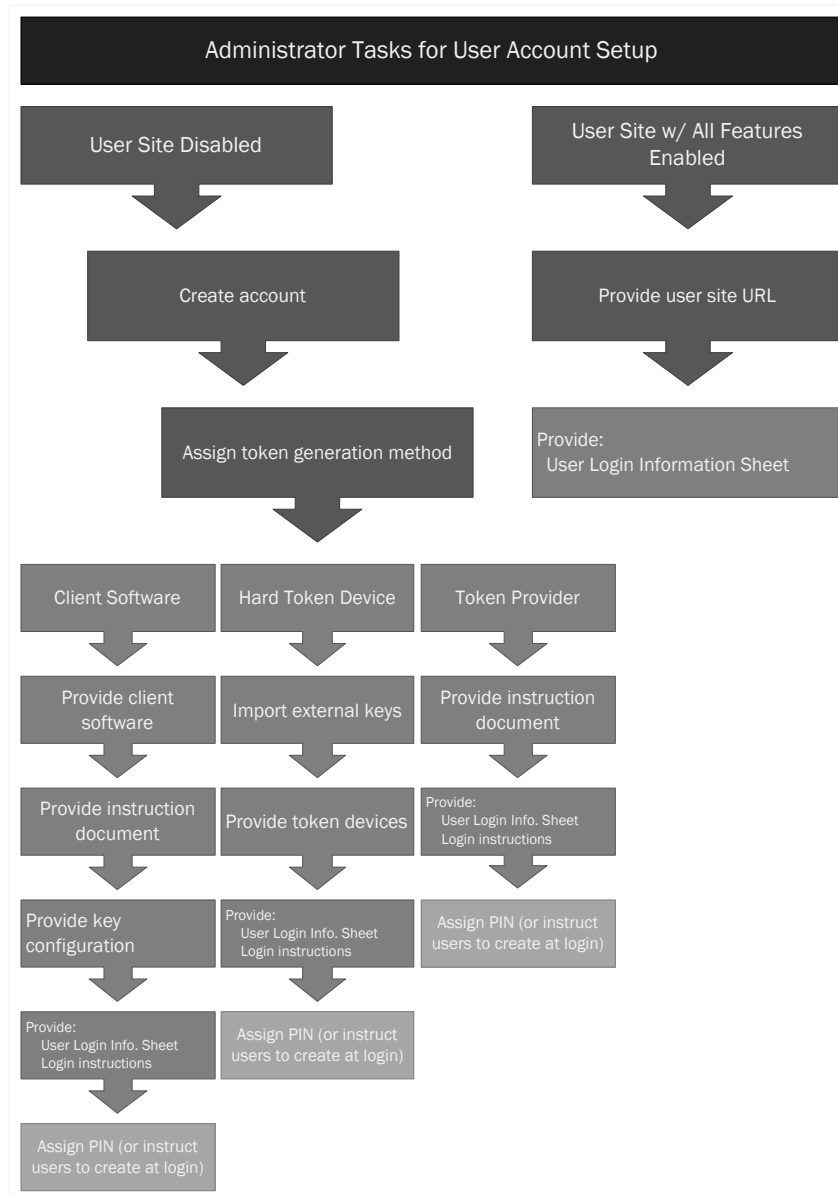


Illustration 6 – User Account Setup Diagram

While enabled features can be more convenient for administrators to manage, your organization’s security/management policies may indicate that some features can be allowed, while others should be disabled.

See the [HOTPIn User Website Notes](#) section below for important information about the user website.

Website Access

Once enabled, default access to the site is:

`https://(appliance host name|IP):8098/hotpin/`

Examples:

`https://acme.com:8098/HOTPin/`

`https://192.168.20.1:8098/HOTPin/`

The site is not enabled by default; it must be turned on by administrators.

Import from Network Feature

The client software Import from Network feature lets users securely import token key configuration from a LAN connection to the user site. This feature requires AD for authorization (as mentioned in previous sections, HOTPin user names must match the AD authentication property). Users need the appliance host name or IP address to download their token key through the client.

Examples:

`hotpinappliance`

`192.168.20.1`

If a user imports the key configuration from a network connection to HOTPin, the default client software settings from the HOTPin Settings page are applied. You can require users to create a key passphrase to protect the key on the user device; this can provide an extra layer of security as a user will be prompted for this passphrase each time they either open the client or load the encrypted key. For more information, see [Configure System Settings](#).

Please Note: The Import from Network feature is disabled for user accounts that are assigned hard tokens and the import will fail if attempted.

User Information

You can provide the addresses for the user site and/or the server to users through the [HOTPin User Login Information Sheet](#).

Manage User Site Settings

The first set of instructions explains how to enable/disable the user website. The second set covers editing user site settings. When managing the site, the Website Settings tab allows you to enable/disable features that allow end users

to manage their HOTPin accounts. The AD Settings tab provides the configuration that allows HOTPin to connect to Active Directory.

To enable the user provisioning website:

1. Navigate to **HOTPin|User Website**.
2. Select **Enable user website** to allow access to the HOTPin User Website.
3. Click **OK** to return to the main HOTPin screen when you are done.

Please Note: To disable the site, deselect the **Enable user website** checkbox. If you disable the user site, the AD Settings tab configuration will be erased.

If all features are enabled, the HOTPin User Website main screen will display similar to the example in Illustration 7 below.

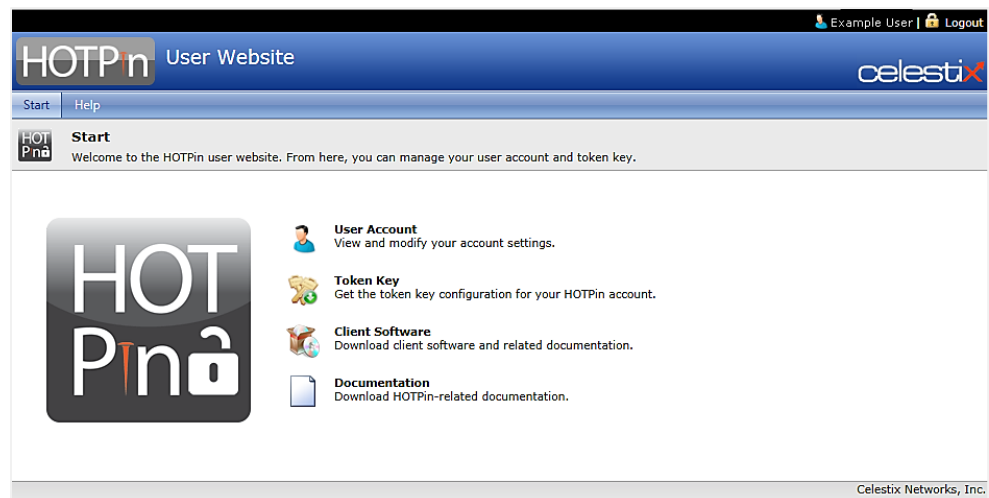


Illustration 7 - HOTPin User Website Fully Enabled

When the HOTPin site is first enabled, all individual functions are enabled by default. Next you should review and adjust configuration on the Website Settings and AD Settings tabs to suit your organization's deployment. For example, if **AD Synchronization** is deployed, you will need to disable end user account creation and edit features. Instructions are covered in the steps that follow, and configuration details are discussed in the subsequent topics.

To edit user website settings:

1. If necessary, navigate to **HOTPin|User Website**.
2. Select one of the following tabs:
 - **Website Settings** – configure user access to the following site features:

- **User Account** – where users view/edit user account information.
- **Token Key** – where users generate a token key configuration to use in client software.
- **Client Software** – where users download client software installation files and instructions.
- **Documentation** – where users access general HOTPin documents.

See [Configure Website Settings](#) for information.

- **AD Settings** – configure HOTPin access to AD. HOTPin uses AD to authenticate valid domain users so they can create accounts or download key configuration through the network. See [Configure AD Settings](#) for information.

3. Click **OK** to return to the main HOTPin screen when you are done.

Configure Website Settings

The following HOTPin User Website properties should be adjusted based on your organization's security and management profile. Illustration 8 provides a reference.

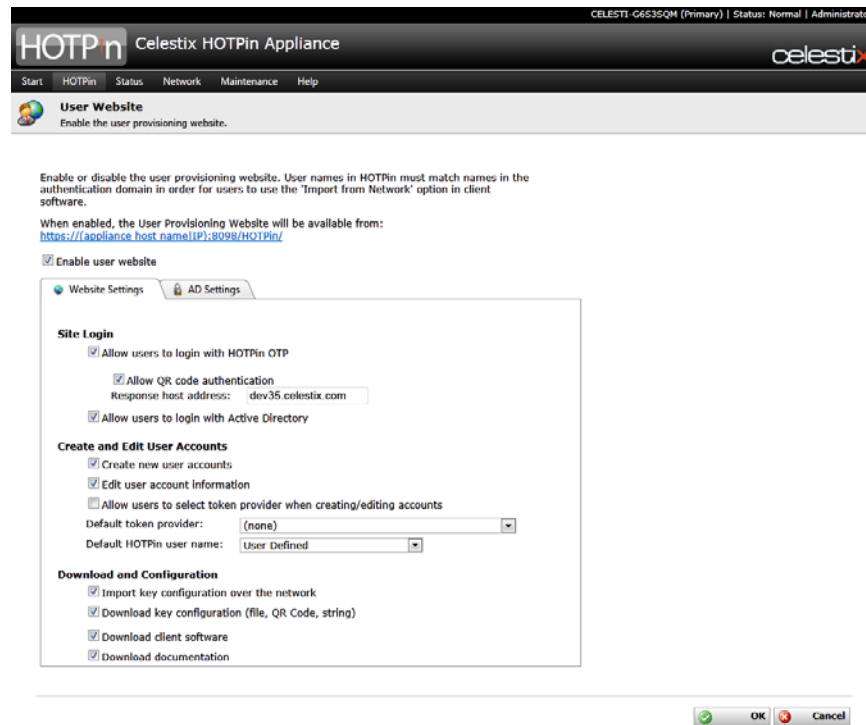


Illustration 8 - Website Settings Tab

If selected, the following properties are enabled:

- **Site Login** – these settings only apply to the HOTPin User Website. Select one or both of the options; selecting both allows the user to choose which to use. Use the [HOTPin User Login Information Sheet](#) to provide users with information about where to access the site.

- ♦ **Allow users to login with HOTPin OTP** – enable login with a HOTPin token code (OTP).
 - **Allow QR code authentication** – enable QR codes that client software can use for login.
 - **Response host address** – optional setting to specify the user website's IP address. The QR login feature will use whatever address is entered into the browser when the QR code is created; this field will override the browser URL and is used in deployments where client software would not be able to resolve the address otherwise. For example, if a NetBIOS name is part of the URL.
Note: If HOTPin **high availability** is deployed, the address specified above must match the primary server address.
- ♦ **Allow users to login with Active Directory** – enable AD authentication for user site access. If users set up their own accounts, they will be assigned a HOTPin user name from the AD authentication property specified in the **Create and Edit User Accounts** **Default HOTPin user name** field.
Important: If AD is not selected, then users cannot create their own accounts. AD is required to authenticate valid domain users.
- **Create and Edit User Accounts** – enable account provisioning/editing functions.
 - ♦ **Create new user accounts** – users with valid AD accounts can create HOTPin accounts. An account can be created to use with either client software or token providers.
 - ♦ **Edit user account information** – users can change account information; if disabled, users can view account information. Must be enabled to allow users to edit token provider/client software option.
 - ♦ **Allow users to select token provider when creating/editing accounts** – if disabled, the **Default token provider** option below will be assigned. If enabled, you will need to tell users if they should select an option different from the default. See **User Login Information**.
 - ♦ **Default token provider** – designates the option that will display when users view/create accounts. If users can edit their token provider/client software option, they can change to any option from the list. If editing is disabled, the method specified here will be assigned to all user generated accounts. The **none** option indicates that client software will be used to generate token codes. Only one token code generation method can be assigned to a HOTPin account.
Note: **External keys** cannot be assigned through the user site; administrators must assign them through the web UI.
 - ♦ **Default HOTPin user name** – select the AD property that HOTPin will assign, or indicate User Defined if only HOTPin authentication will be used.
- **Download and Configuration** – enable client software setup functions.

- **Import key configuration over the network** – required for the client software Import from Network function. This feature is not visible on the user website; it requires valid AD credentials and a network connection.
- **Download key configuration (key, QR code, string)** – required to allow users to get key configuration; users select an option compatible with their client device.
- **Download client software** – required to allow users to get their own client software; some apps, however, are only available from download sites associated with the device platform; iOS and Android are examples. Most of the common mobile devices have client software available. Instructions for how to install and use client software are included for all supported device platforms and are listed by device.
- **Download documentation** – allows users to access general documentation like login instructions for both the client software and provider token code generation methods.

Configure AD Settings

The following AD information is required to allow users to provision their own accounts, client applications, and/or to download key configuration over the network. Illustration 9 provides a reference.

The screenshot shows the 'User Website' configuration page for the Celestix HOTPin Appliance. The 'AD Settings' tab is selected. The page includes instructions on enabling the user provisioning website and a link to its URL. Below this, there are checkboxes for 'Enable user website' and 'Validate the server settings before saving'. The 'Validate' checkbox is checked. Fields for 'Primary server IP address/host' (10.19.19.1) and 'Secondary server IP address/host' are present. A dropdown menu for 'Authenticate against' is set to 'Active Directory (LDAP)'. There is also a 'Group membership' field. A section for 'Authenticate with user email address' includes a checkbox (unchecked) and a note to specify credentials to the server to retrieve user email address with. Fields for 'User (domain\user):' and 'Password:' are provided. At the bottom right, there are 'OK' and 'Cancel' buttons.

Illustration 9 - AD Settings Tab

Enter the following settings to configure access to AD:

- **Validate the server settings before saving** – select to test the AD settings that follow.

Note: Validation occurs when you click the OK button after configuring settings.

- **Primary server IP address/host** – enter AD server information.
- **Secondary server IP address/host** – optional; enter information for an additional AD server.
- **Authenticate against** – select the authentication service type.
- **Group membership** – optional; this feature can be used to restrict end user access to self-provisioning functionality. If you enter a group name, only members of that group will be able to use HOTPin.
- **Authenticate with user email address** – select to enable HOTPin to get user email addresses from AD in the authorization process. This will allow end users to enter their email address as the user name when they import key configuration. You will need to enter a **User (domain\user)** name and **Password** with AD read privileges.

Important:

- › Email addresses must be entered in the AD user account email attribute and must also be unique values.
- › If you select **Authenticate with user email address**, you should designate **Email Address** as the **Default HOTPin user name** on the **Website Settings** tab.

AD Synchronization Compatibility

If you deploy both the **AD Synchronization** and HOTPin User Website features, you should limit end user editing functionality to avoid issues where the sync process overwrites information they might enter. Disable the following user site features under **Create and Edit User Accounts**:

- Create new user accounts
- Edit user account information

User Website Notes

- You might need to adjust the appliance firewall settings to allow users to connect to the user provisioning website; depending on your deployment, this may include the Windows Firewall, TMG, or an external firewall.
- If the website is disabled, attempts to use the Import from Network feature in client software will generate an unauthorized access error message.
- The network import option in client software requires that HOTPin user names match the user's domain authentication property (based on the configured settings as discussed above).
- Some client software is available from the user site for download, but some applications must be downloaded from the site associated with

the platform (for example, the iOS client must be downloaded from Apple's App Store).

- The user provisioning website must be enabled to support end users with iOS client software versions prior to 3.0 as they can only import token key configuration through the network.
- A user account must be enabled to allow users to log in to the user site.

Configure AD Synchronization

Synchronization allows administrators to link the HOTPin user database to Active Directory (AD) user account information. This simplifies user management because accounts are automatically updated, including HOTPin account creation and deletion. The sync feature is a one-way update, where HOTPin information is updated with run-time AD account data. Once configured, synchronization will continue running in the background.

Important:

- › Deploying synchronization makes the HOTPin user database dependent on AD accounts. [Synchronization Overview](#) provides more information.
- › If you will deploy both AD Synchronization and the HOTPin User Website, you should consult the [HOTPin User Website Compatibility](#) topic below for more information. Syncing will affect its functionality.

To access the synchronization tool:

1. Navigate to **HOTPin|AD Synchronization**.
2. Click **Next** on the Welcome screen to start the wizard.

The wizard guides you through the steps to set up syncing. Illustration 10 provides a reference for the AD Synchronization screen.

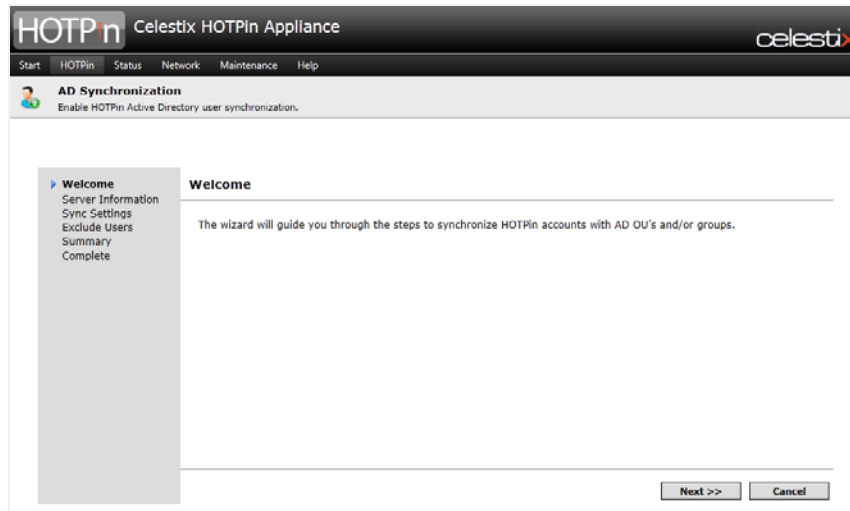


Illustration 10 - AD Synchronization Screen

The following topics provide an overview to explain automatic user account management through synchronization, and instructions for the wizard.

Synchronization Overview

The overview first covers the exclusion list, a synchronization process component that informs how you will deploy syncing. Then the process functionality is broken down to show what HOTPin links to, and what results occur during synchronization after changes are made to either HOTPin or AD accounts.

Exclusion List

The exclusion list allows administrators to designate accounts that do not participate in the sync process. You can include both AD and HOTPin accounts:

- Designate AD accounts that you do not want to import.
- Designate AD accounts that have been imported, but that should not be changed subsequently (requires running the tool after AD accounts have been added).
- Designate HOTPin accounts that do not exist in AD.

Excluding AD accounts that aren't used for authentication is important to preserves space in the HOTPin user license limit.

Important: HOTPin accounts added to the system through the web UI's Users feature (either manually or through import), must then be noted in

the exclusion list; otherwise they will be deleted after the next sync interval.

Sync Process Functionality

To set up synchronization you will need to understand how HOTPin links to AD, and how administrative actions result in changes to the HOTPin database.

Active Directory/HOTPin Synchronization Links

The following table explains the relationship between AD and HOTPin accounts. It illustrates the required information that AD properties must contain to populate HOTPin fields.

HOTPin Field (General Tab)	AD Property (Tab/Field)
User name	Account/User logon name (Domain, SAM Account Name, UPN) -or- General/E-mail
Full name	General/Display name
Description	General/Description
Email	*General/Email
Phone	*General/Telephone number
* Only required if needed for a token provider deployment; these field updates must be enabled in Sync Settings.	

Unless an account is noted in the exclusion list, changes made to these AD fields are then updated in the correlating HOTPin fields after the next sync interval.

Important: In the HOTPin system, the phone number is used to send SMS messages containing a token code. Thus the AD telephone number field should contain mobile phone information.

Synchronization Results

To help illustrate the process, the following table describes some account actions and resulting sync operation effects to HOTPin accounts. It includes actions with potentially unintended results for a more complete view of the process.

If an account in AD is:	The sync update action in HOTPin will be:	If an account in HOTPin is:
Added	Account added	
Deleted	*Account deleted	
	No sync action, account remains	Account added & noted in exclusion list
	*Account deleted	Account added & <u>not</u> noted in exclusion list
	No sync action, account still deleted	HOTPin account noted in exclusion is deleted
	No sync action, account still deleted (and still in the exclusion list)	AD-linked account noted in exclusion list is deleted
	Account is added	AD-linked account deleted
* Deleted unless Sync Settings are configured to disable accounts in HOTPin.		

Please Note: The table above is illustrative and not intended to represent the spectrum of sync actions.

Synchronization Wizard Instructions

1. Navigate to **HOTPin|AD Synchronization**.
The **Welcome** screen opens.
2. Click **Next**.
3. On the **Server Information** screen, complete the following:

- a. **Enable AD synchronization** – select.
- b. **Primary server IP address/host** – enter an IP or host name for your main AD server.
- c. **Secondary server IP address/host** – enter an IP or host name if your deployment includes an additional server for AD.
- d. **User (domain\user)/Password** – enter credentials for an account with administrator privileges for AD.

4. Click **Next**.
5. On the **Sync Settings** screen, complete the following to add/update user accounts:

Sync Settings

Welcome
Server Information
Sync Settings
Exclude Users
Summary
Complete

Select OUs
Select Groups

AD property for account name: SAM account name
Token provider: (none)
☐ Update e-mail and phone
Sync interval: 15 minutes
If AD account is missing: Delete user from HOTPin

<< Previous Next >> Cancel

Note: At least one OU or group must be selected.

- a. **Select OU** – click to access the list of Organizational Units:

- Select checkboxes to add.
- Click **OK**.

- b. **Select Groups** – click to access a list of AD groups:

Note: The wizard hides built-in groups by default; select **Show Built-in Groups** to display those options.

- Select checkboxes to add.
- Click **OK**.

- c. **AD property for account name** – select the property to assign for HOTPin user names.

- d. **Token provider** – designate the token code generation option that will be assigned to new accounts; **none** will assign client software as the method.

Note: An **external key** will need to be individually assigned to user accounts.

- e. **Update email and mobile phone** – select to sync AD email and telephone number properties to HOTPin accounts.

Note: An AD email or phone property will be required if a token provider is assigned as the token code generation method.

- f. **Sync interval** – select the frequency in which HOTPin will seek updates from AD.

- g. **If AD account is missing** – select the action HOTPin will take if a user account has been deleted from AD:

- **Delete user from HOTPin**

Note: Once a HOTPin user is deleted, the action cannot be undone.

- **Disable user in HOTPin**

Note: Disabled accounts count towards the user license limit.

6. Click **Next**.
7. On the **Exclude Users** screen, you will designate AD accounts that should not be added/changed in HOTPin, and/or HOTPin accounts that are not based on AD accounts. Complete the following:

The screenshot shows the 'Exclude Users' configuration window. On the left is a sidebar with a menu containing 'Welcome', 'Server Information', 'Sync Settings', 'Exclude Users' (highlighted with a blue arrow), 'Summary', and 'Complete'. The main content area is titled 'Exclude Users'. It features a checked checkbox labeled 'Exclude these accounts from Sync'. Below this is a large empty rectangular box, likely for a list of users. To the right of this box are two buttons: 'Exclude AD Users' and 'Exclude HOTPin Users'. A yellow warning box with a document icon contains the text: 'Important: HOTPin accounts not in common with AD will be deleted if not excluded from syncing.' At the bottom right of the window are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

- a. **Exclude these usernames from Sync** – select to enable the exclude function.
 - b. **Exclude AD Users** – click to access the list of AD users:
 - Select checkboxes for accounts to exclude.
 - Click **OK**.

Note: Select this option to add accounts that exist in synced AD OUs/groups, but should either not be added if you are importing accounts, or subsequently changed if you are editing sync settings.
 - c. **Exclude HOTPin Users** – click to access the list of HOTPin users:
 - Select checkboxes for accounts to exclude.
 - Click **OK**.

Note: HOTPin accounts that do not exist in the synced AD OUs/groups must be noted here, or they will be deleted.
8. Click **Next**.
 9. Review the **Summary** screen before committing the settings.

Click the **Previous** button to return to an earlier screen to adjust settings.
 10. Click **Finish** to commit configuration.
 11. Click **Close** on the successful synchronization prompt and return to the main HOTPin screen.

Once you have configured settings, users will be added to HOTPin after the next sync interval. To add accounts to HOTPin immediately, you will next need to use the **manual sync tool**.

HOTPin User Website Compatibility

If you deploy both the AD Synchronization and **HOTPin User Website** features, you should limit end user editing functionality to avoid issues where the sync process overwrites information they might enter. Disable the following user website features under **Create and Edit User Accounts**:

- Create new user accounts
- Edit user account information

Please Note: End-user edited accounts noted on the exclusion list would not be overwritten; however, as you cannot enable editing for individuals or groups on the user site, you should disable the functionality to avoid issues.

Manual Sync

The Manual Sync feature is an on-demand synchronization tool. It immediately updates HOTPin user accounts with run-time AD account data for synced OUs and groups.

Please Note: Synchronization settings must be configured through the wizard before you can use on-demand syncing (see [Synchronization Wizard Instructions](#)).

Illustration 11 provides a reference for the wizard's Manual Sync feature.



Illustration 11 - Manual Sync Wizard Screen

To sync HOTPin on demand:

1. Navigate to **HOTPin|AD Synchronization**.

2. Select **Manual Sync**.
3. Click **Next**.
4. Click **Finish**.
5. Synchronization results are displayed. See [Synchronization Result Details](#) below for information.
6. Click **Close** to return to the HOTPin screen.

Synchronization Result Details

- **User Name** – lists HOTPin user name.
- **Full Name** – displays descriptive name; usually first and last.
- **Sync Status** – displays sync outcome.
- **Sync Type** – differentiates the sync action executed:
 - ♦ **Create**
 - ♦ **Update**
 - ♦ **Disable**
 - ♦ **Delete**

Import External Token Keys

The Token Keys screen provides access to external key configuration. External keys are currently used in hard token devices to create codes for user authentication. An external key is imported to HOTPin and then assigned to a user account; then the codes produced by the corresponding device can be used for login. This provides another option to generate token codes for authentication apart from the HOTPin-defined keys used in client software or token providers.

Please Note: To maintain synchronization with the server, a user should only use one token generation method – client software (the default), an external key, or a token provider.

To access the token key screen:

1. Navigate to **HOTPin|Token Keys**.
2. View or import keys.
3. Click the **Close** button to return to the main HOTPin screen.

Illustration 12 provides a reference for the Token Keys screen.

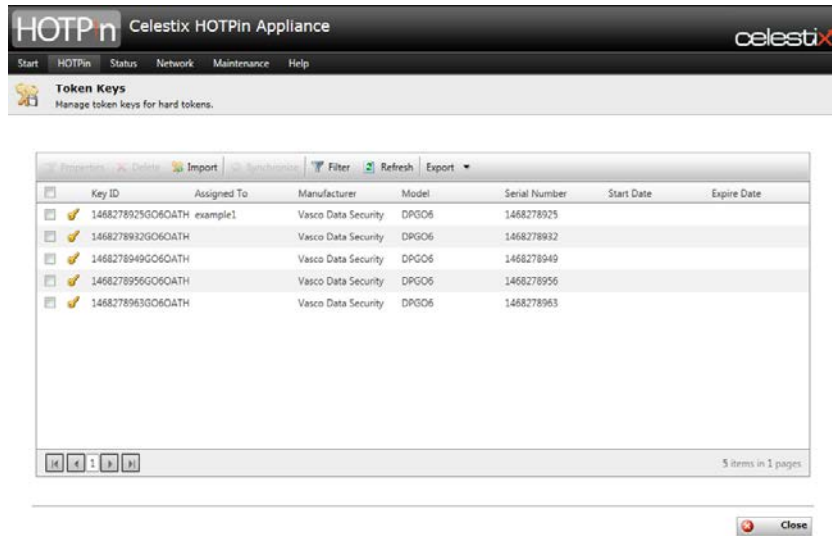


Illustration 12 - Token Keys Screen

The token keys list provides the following summary information:

- **Key ID** – differentiates the key the device uses.
- **Assigned To** – lists the key’s designated user account.
- **Manufacturer** – identifies the hard token maker.
- **Model** – identifies the token device.
- **Serial Number** – unique identifier for the token device.
- **Start Date** – if included, displays the date the device is valid from.
- **Expire Date** – if included, displays the date the device is valid until.

Please Note: Device keys must be globally unique; the key ID, manufacturer, model, and serial number can all be used to help differentiate keys.

Illustration 13 provides a reference for the key import screen.

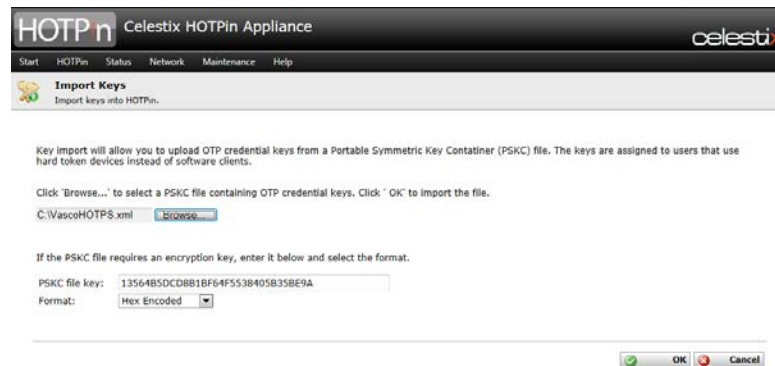


Illustration 13 - Import Keys Screen

Please Note: The import function uses an OATH-compliant Portable Symmetric Key Container (PSKC) file that contains information to populate the token keys list.

To import external keys:

1. If necessary, navigate to **HOTPin|Token Keys**.
2. Click **Import**.
3. Complete the following:
 - a. **Browse** – click to navigate to and select the PSKC file.
 - b. **PSKC file key** – if required, enter the key used to encrypt the file.
 - c. **Format** – if required, select the key's encryption format:
 - **Plain Text**
 - **Hex Encoded**
 - **Base64 Encoded**
4. Click **OK**.

Successful import is noted on the Import Keys screen.
5. Click **OK** to return the Token Keys screen.

Only administrators can assign or manage external token keys. If an external key is assigned, downloading keys will be disabled for the account. For instructions, see [Assign an External Key to a User Account](#).

Configure Token Providers

Token providers are HOTPin system add-ins that send a user the next valid token code for authentication. They accommodate users who do not have either a hard token or user device that can run client software.

If you are not familiar with the potential security issues posed by choosing a token provider instead of the client software, please see the [Token Provider Security Considerations](#) section below.

The following reference information is available on the Providers screen:

- **ID** – token provider identifier; use this when assigning a token method to users through the [Import Users](#) feature.
- **Title** – token provider name.
- **Version** – HOTPin application information.
- **Description** – token provider function explanation.

To access token provider properties:

1. Navigate to **HOTPin|Providers**.
2. Select a provider from the list.
3. Click **Properties**.

Properties will vary among the different providers. See the individual provider's section for details about configuration.

Provider Security Considerations

This section discusses some issues that system administrators should review when considering the use of token providers in a HOTPin system deployment. You should evaluate the risks to determine whether provider options are acceptable for your organization.

A token provider is as secure as the encryption method for the technology being used. If email is sent in plain text, or the HTTP provider is not deployed with SSL/TLS, then the sent token code is vulnerable. Both email and HTTP traffic can be sniffed or intercepted while traveling over the Internet; you should consider whether using HTTPS options provide the necessary level of security. SMS messages are handled by third-party service carriers and you should review the technology for any issues that may compromise secure access to your network resources.

Please Note: To use a stolen code, the malicious user would need to know where to log in as well as the user name and PIN* for the account the intercepted code belongs to (*if PIN requirement is enabled).

To decrease potential risk for provider options, the next available token code is:

- Sent only once to the user.
- Valid for a limited amount of time. See Configure System Settings : **Token Provider** for **Sent Code TTL** (time to live).

It is also important to note that the loss of a single token code does not compromise the system as it does not provide information that would allow a hacker to guess the next token value. A lost user device with active client software, for example, does represent a security issue (thus for client software deployments, users should be instructed to report lost devices immediately).

System administrators can also improve security by incrementing a user's authentication failure counter each time a token provider sends the user a token code. When the maximum is reached the account is locked out (see **Configure System Settings : Authentication : Maximum Authentication Failures**).

Test Provider Feature

Each of the providers described in subsequent sections has a test feature that allows you to check the configuration you enter. It sends a code using the information you enter in the test tool, which allows you to check provider configuration without requiring valid HOTPin user data.

Please Note: While either phone or email information is required, other fields are optional.

To test provider application settings:

1. Expand the debugging tool by clicking **Test Provider**.
2. Enter user information in the following fields:

Note: the **Code** item is a static value for the OTP that will be included in the test message. It is not valid for authentication.

- **User name** – optional; enter a user name to include in your test sample.
- **Full name** – optional; enter an example name to include in your test sample.
- **Email** – enter an email address if testing the Email OTP Provider.

Note: You can also test an email-to-SMS address in this field.

- **Phone** – enter a mobile phone number if testing the SMS OTP Provider.
3. Click **Send Test User Information**.

A message on the provider's screen will indicate if the code was successfully sent.

Token Provider Options

The following sections explain how to access and configure HOTPin token provider options. You only need to configure the providers your organization will use. It will help to consider how you will implement the token provider before you import/add users as that will affect whether you need to enter their email and phone information.

Each provider topic includes a Settings and Customizable Fields section. Customizable fields allow you to configure the information the provider sends. You will enter information that pertains to your organization, though some fields contain default entries that may be helpful for your deployment. Replaceable tags are used in the provider settings to call current user information that will then be included in sent token code messages. These code tags combine with

static information to adapt customizable fields as necessary. Replaceable tags are defined in braces { } and available options are noted in each of the provider sections.

Configure the Email OTP Token Provider

The Email OTP Token Provider sends the next valid token code to a standard email address or an email-to-SMS address (text message).

To access email provider properties:

1. Navigate to **HOTPin|Providers**.
2. Select the **Email OTP Provider** from the list.
3. Click **Properties** to open the provider configuration screen.
4. Click **OK** to save the settings you entered.

The following subsections explain the settings on the Provider Properties page. Illustration 14 provides a reference.

Illustration 14 - Email OTP Provider Properties

Settings and Customizable Fields:

- **To** – addressing information; the default is the {email} tag, which is replaced with the email address defined for the user.
- **From** – the sender address should be a valid account on the server that is listed in the **Email server address** field below.

- **Subject** – identifies the message; **HOTPin OTP** is the default static text.
- **Message** – message content; usually contains at least the {code} tag, which will be replaced with the current token code when HOTPin sends the message to the user.

Replaceable Tags for the To, Subject, and Message fields:

- **{user_name}** – the user's login name.
- **{user_full_name}** – the user's full name.
- **{email}** – the user's email address.
- **{phone}** – the user's phone number.
- **{code}** – the next token code.
- **{timestamp}** – the date and time the request was sent to the provider.

Important: Without the {code} tag included in the Subject or Message field, the message will not provide a token code to the user.

- **Email server address** – enter the mail server name or IP address.
- **Port** – enter the mail server port number.
- **Connect using SSL** – select the protocol your mail server uses.
- **Use email server authentication** – select if necessary for your email server and include credential information (**User name, Domain, Password**) if required.

See the previous section [Test Provider Feature](#) for information about using the tool to check the configuration you entered. If you do not receive the test OTP, try the following troubleshooting steps:

- Confirm your provider configuration.
- Check the user information you entered.

For more information about token provider settings, see Configure System Settings : [Token Provider](#).

Configure the HTTP OTP Token Provider

The HTTP OTP Token Provider sends the next valid token code to a predefined URL via HTTP or HTTPS. The URL is configured with special tags that are replaced with a user's current values to produce a URL with unique query variables (for example, `http://host/?phone={phone}&code={code}`). This provider is generally used to send the code to an SMS server that will then send it to a user's mobile phone.

To access HTTP provider properties:

1. Navigate to **HOTPin|Providers**.
2. Select the **HTTP OTP Provider** from the list.
3. Click **Properties** to open the provider configuration screen.
4. Click **OK** to save the settings you entered.

The following subsections explain the items on the Provider Properties page. Illustration 15 provides a reference.



Illustration 15 - HTTP OTP Provider Properties

Settings and Customizable Fields:

In the Website URL field, enter the information required by your service provider along with replaceable tags for the HOTPin information you want to include in the sent code message.

- **Website URL** – the URL property defines the host and query string where the next token code will be sent. The query string should include special tags that are replaced with runtime values when the HTTP OTP Token Provider sends the next code. Any special characters included in the query variables must be in URL-encoded format; for example, a space should be written as %20; double quotes as %22.

Replaceable Tags for the URL field:

- **{user_name}** – the user's login name.
- **{user_full_name}** – the user's full name.
- **{email}** – the user's email address.
- **{phone}** – the user's phone number.
- **{code}** – the next token code.
- **{timestamp}** – the date and time the request was sent to the provider.

Important: Without the {code} tag included in the Subject or Message field, the message will not provide a token code to the user.

URL Examples:

The URL field format may vary, depending on the server requirements for the web or SMS application that processes the token code information. The following examples illustrate possible formats as a point of reference.

HTTP samples:

```
http://sms.server.com/service.aspx?ph={phone}&text={code}
```

```
http://sms.server.com/service.aspx?ph={phone}&text=Token%20code%20{code}
```

```
http://10.1.1.1:2000/service.aspx?ph={phone}&text={code}
```

Secure sample passing a service login user name and password with token information:

```
https://sms.server.com/service.aspx?user=admin&pwd=123456&ph={phone}&text={code}
```

- **Log the website response HTML for debugging** – a tool to help system administrators debug HTTP provider operation by logging the returned HTML pages from the web server to HTTP provider log files (**HOTPin|Log Files**). This should only be used as a temporary debugging tool because one response is logged for each token code request.
- **Use a proxy server to access website** – enable a proxy server to send token code messages and include the necessary information below.
 - ♦ **Server address** – specify the proxy server address.
 - ♦ **Server port** – specify the server port to use.
 - ♦ **Bypass proxy on local address** – select to bypass the proxy server for local addresses.
 - ♦ **Set proxy server credentials** – select to enable and include credential information (**Proxy server user, Domain, Password**) if required.

See the previous section **Test Provider Feature** for information about using the tool to check the configuration you entered. If you do not receive the test OTP, try the following troubleshooting steps:

- Confirm your provider configuration.
- Check the user information you entered.
- Check firewall settings; depending on your deployment, this may include the Windows Firewall, TMG, or an external firewall.

For more information about token provider settings, see Configure System Settings : **Token Provider**.

Configure the SMS OTP Token Provider

The SMS OTP Token Provider sends a token code to a mobile phone via a GSM/GPRS Serial or USB Modem connected directly to your appliance. The provider only connects to the modem when sending a message; it disconnects when finished.

To access SMS provider properties:

1. Navigate to **HOTPin|Providers**.
2. Select the **SMS OTP Provider** from the list.
3. Click **Properties** to open the provider configuration screen.
4. Click **OK** to save the settings you entered.

The following subsections explain the items on the Provider Properties page. Illustration 16 provides a reference.

The screenshot shows the 'SMS OTP Provider' configuration window in the HOTPin Celestix HOTPin Appliance. The window has a title bar with 'HOTPin' and 'Celestix HOTPin Appliance' on the left, and the 'celestix' logo on the right. Below the title bar is a navigation menu with 'Start', 'HOTPin', 'Status', 'Network', 'Maintenance', and 'Help'. The main content area is titled 'SMS OTP Provider' and includes a description: 'This provider will send the token code to a mobile phone via a directly connected GSM/GPRS Serial or USB Modem.' Below this, there's a section for 'Communication Settings' with fields for 'COM port' (set to COM1), 'Stop bits' (set to 1), 'Baud rate' (set to 115200), 'Handshake' (set to None), 'Parity' (set to None), 'Timeout (milliseconds)' (set to 3000), and 'Data bits' (set to 8). There's also a checkbox for 'RTS enabled' which is checked. Below the communication settings is a section for 'AT Commands' with a text area containing the following commands: 'AT+CM3P=1', 'AT+CM3S=""(phone)"', and 'Token code: {code} {eof}'. There's a checkbox for 'Log the modem response for debugging' which is unchecked. At the bottom right of the main content area is a 'Reset to Defaults' button. Below the main content area is a 'Test Provider' button. At the very bottom of the window are 'OK' and 'Cancel' buttons.

Illustration 16 - SMS OTP Provider Properties

Settings and Customizable Fields:

▪ Communication Settings

This property defines how the provider communicates with the modem attached to your appliance. The provider includes default configuration that may work for your system, but you should consult your modem's documentation for definitive connection settings. Properties include:

- ♦ **COM port** – enter the communication serial port number, physical or virtual, that the modem is connected to (see [COM Port Locations](#) for information).
- ♦ **Stop bits** – enter the number of stop bits per byte.
- ♦ **Baud rate** – enter the serial port baud rate.
- ♦ **Handshake** – indicate the handshaking protocol for serial port transmission of data.
- ♦ **Parity** – indicate the parity-checking protocol.
- ♦ **Timeout (milliseconds)** – enter the maximum amount of time in milliseconds the provider will wait to get a response from the modem. This value must be between 100 (one-tenth of second)

and 30000 (30 seconds). Depending on the modem speed, this value may need to be adjusted to prevent timeout errors.

- **Data bits** – indicate the standard length of data bits per byte.
- **RTS enabled** – designate whether the Request to Send (RTS) signal is enabled during serial communication.

- **AT Commands**

To send an SMS Message to the modem, configure the proper AT commands; each command must be on a separate line. Refer to your modem documentation for more information about AT commands if you need to adjust the suggested settings. The default commands are:

- **AT+CMGF=1** – configure text message format.
- **AT+CMGS="{phone}"** – phone number to send the message to.
- **Token code: {code} {eof}** – message string followed by the end-of-file character.

In the default settings, the SMS provider uses the replaceable tags '{phone}', '{code}' and '{eof}' in the **AT Commands** property to inject the user's phone number, current OTP and the required end-of-file character into commands that are sent to the modem. These tags are required for the SMS Provider to function. The replaceable tags listed below can be used to include additional information in the SMS message.

Replaceable tags for AT commands:

- **{user_name}** – the user's login name.
- **{user_full_name}** – the user's full name.
- **{email}** – the user's email address.
- **{phone}** – the user's phone number.
- **{code}** – the next token code.
- **{timestamp}** – the date and time the request was sent to the provider.

Important: Without the {code} tag included, the message will not provide a token code to the user.

- **Log the modem response for debugging** – a tool to help system administrators debug SMS provider operation by logging modem traffic to SMS provider log files (**HOTPin|Log Files**). This should only be used as a temporary debugging tool because one response is logged for each token code request.
- **Reset to Defaults** – restore properties in the **Communication Settings** and **AT Commands** sections to the original settings.

COM Port Locations

Most GPRS/GSM modems will communicate over a USB or serial cable and can connect to any like port that is open on the appliance; the Windows operating system will define a virtual COM port for USB devices. Available connections will be listed under **Communication Settings** in the **COM port** drop menu.

See the previous section [Test Provider Feature](#) for information about using the tool to check the configuration you entered. If you do not receive the test OTP, try the following troubleshooting steps:

- Confirm your provider configuration.
- Check the user information you entered.

For more information about token provider settings, see Configure System Settings : [Token Provider](#).

The Next Step

Now that you have configured your appliance and the HOTPin server application, user accounts must be added if you did not sync HOTPin with AD or enable the user site. The following user accounts section provides information about:

- [User property settings](#).
- How to [import](#) or [add](#) users.
- How to download [client software](#) and [token keys](#) for end users.

HOTPin User Accounts

The HOTPin user information database is accessed through the Users section in the appliance web user interface. Each user has associated information such as login name, email address and token key. There are multiple ways to add user accounts, which include:

- A. Synchronizing with AD
- B. Users self-provisioning through the HOTPin User Website
- C. Importing from AD or a text file through the web UI
- D. Adding individually through the web UI

Synchronization with AD can be the simplest way to maintain HOTPin user accounts, but it affects the self-provisioning functionality of the HOTPin User Website. Fully enabling the **HOTPin User Website** allows users to provision accounts for either token provider or client software token generation methods, and it also allows users to set up client software. If you choose not to sync with AD nor to enable the user site, then you will either import accounts from Active Directory or a text file, or add them manually through the web UI.

Please Note: If using options A, C, or D, it will be necessary to provide client installation and token key configuration files to users in client software deployments. The user site can be enabled to allow those features without enabling self-provisioning.

This section provides instructions for manually adding user accounts, accessing client software, and downloading user token keys. Also, to add users efficiently, it will be helpful if you consider how the information will be used prior to adding or importing them. For example, token providers rely on user email addresses or phone numbers to send token codes. Thus, if token providers are included in your deployment, that information would need to be included when user accounts are created.

Manage User Accounts

From the Users screen, accounts can be added manually or imported from a text file or Active Directory (AD). The following topics cover user property settings, adding/editing users individually, and both import methods. Then, instructions to add external keys to HOTPin accounts that will use hard tokens are covered.

Please Note: In AD domains, HOTPin user names should be the same as the AD authentication property. See [Active Directory](#) for more information.

To access the user management settings and features:

1. Navigate to **HOTPin|Users**.
2. Select a user by clicking the checkbox in the corresponding row.
3. Click the **Close** button to return to the main HOTPin screen.

Illustration 17 provides a reference for the Users screen.

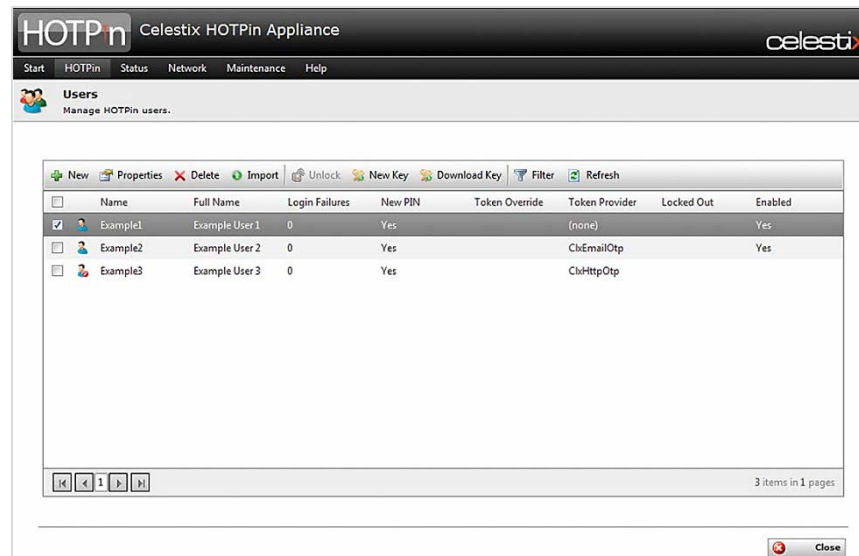


Illustration 17 – HOTPin Users

The Users screen in the web user interface lists all accounts and includes the following information:

- **Name** – the user name; enter 4-128 characters, no spaces.
- **Full Name** – the user's first and last name.
- **Login Failures** – displays the user's total failed attempts to login to your protected system.
- **New PIN – Yes** indicates the user account will be required to create a PIN at the next login.

- **Token Override – Yes** indicates the user account can log in without a token code.
- **Token Provider** – displays the token method assigned to the user account.
 - Note:** Your organization may have had additional customized options created
 - **(none)** – indicates that users will either run client software on a user device (for example: mobile phone, PC) or use an external key (like a key fob hard token).
 - Note:** An external key can only be assigned by an administrator.
 - **ClxEmailOtp** – uses email or email-to-SMS to send a token code to the user.
 - **ClxHttpOtp** – generally used to send the code to an SMS server that will then send it to a user's mobile device.
 - ClxSmsOtp** – sends the code to a user's mobile device through an SMS modem that you connect to your appliance.
- **Locked Out – Yes** indicates the user has exceeded the maximum authentication failures limit (**HOTPin|Settings|Authentication**).
- **Enabled – Yes** indicates the user account is active and has login privileges.

Access these task functions on the Users screen:

- **New** – create a new HOTPin user manually. See the [Add a User](#) topic for more information.
- **Properties** – edit an existing user; select one or multiple users to enable. See the [Change User Account Settings](#) topic for more information.
- **Delete** – remove user accounts; select one or multiple users to enable. This action is not reversible. If the user may need access again, you can disable the account (**HOTPin|Users|Properties|General|Account is enabled**).
- **Import** – add users from AD or a text file through an import wizard. See the [Import Users](#) topic for more information.
- **Unlock** – enable access for users who have exceeded the maximum authentication failures limit (**HOTPin|Settings|Authentication**). Select a user account that has been locked out to enable the button.
 - Note:** Successful authentication will reset the authentication failure counter.
- **New Key** – create a new token key for a user account. Select one or multiple user accounts to enable.

Notes:

- › If the account has now been assigned the client software token generation method, the new token will need to be imported to the user's device.
- › If the account had been assigned an external key, it will be unassigned and then an internal key will be applied.

- Creating a new key removes the user's PIN; when PIN's are required, users will need to reset them.

- **Download Key** – download or copy a user's token key to a local computer as either a file, a QR code, or a string. See the [Download Key](#) topic for more information.

Note: Key import methods vary by client device. See the device-specific instructions for available import methods.

- **Filter** – enter criteria to selectively view list.
 - ♦ Click to open and close filter options.
 - ♦ Click the filter icon for more options; select **NoFilter** to remove.
- **Refresh** – click to see changes to the user list.

Please Note: The HOTPin system includes a [User Login Information Sheet](#) to help you organize the information you will need to provide to your end users. Access the form at **HOTPin|Documentation**.

Add a User

This section provides details for manually adding a user account. Illustration 18 provides a reference.

Illustration 18 - New User Settings

Important: If AD Synchronization is deployed, any accounts added manually through the web UI must be added to the exclusion list, or they will be automatically deleted after the next sync interval.

To add new users:

1. Navigate to **HOTPin|Users**.
2. Click **New**.
3. The **New User** screen opens.
4. Enter user information. See **New User Property Settings** below for information.
5. Click the **OK** button to finish adding a user and return to the **Users** screen.

Important: You will not be able to add more users than are allowed by your user **license**.

New User Property Settings

- **User name** – the user name should be between 4 and 128 characters and cannot include spaces.
Note: In AD domains, HOTPin user names should be the same as the AD authentication property. See **Active Directory** for more information.
- **Full name** – the account holder's name; usually displays first and last.
- **Description** – optional notes for the user account.
- **Email** – the user's standard email or email-to-SMS address. The email address field is optional but may be needed by custom token providers. The value in this field is called by the {email} replaceable tag (see **Token Provider Options**).
Note: Many mobile phone service providers allow SMS messages to be sent from emails. The address is usually the mobile phone number and specific provider domain. For example, a mobile phone number that is 5551112222 and uses AT&T's service would use *5551112222@txt.att.net* as the email-to-SMS address. Check with the user's phone service provider for more information about sending SMS messages by email.
- **Phone** – the user's mobile phone number. This field is optional but may be needed by custom token providers. The value in this field is called by the {phone} replaceable tag (see **Token Provider Options**).
- **Account is enabled** – a check means the account is active; uncheck to disable the account.
Note: Disabled accounts count toward the user license limit.
- **Token Key** – select a key type:
 - **Use internal token key** – select for accounts that will use client software or a token provider.
 - **Token provider** – select one of the options in the drop list. The standard options include:
 - **(none)** – requires that users run a software application on a client device (e.g., mobile

phone, PC) unless an external key is then assigned.

- **OTP Email Provider** – uses email or email-to-SMS to send the token code to the user.
- **OTP HTTP Provider** – generally used to send the code to an SMS server that will then send it to a user's mobile device.
- **OTP SMS Provider** – sends the code through an SMS modem connected to your appliance that will then send it to a user's mobile device.

Your organization may have had additional options created.

- ♦ **Use external token key** – select for accounts that will use an imported key, like a hard token device.
 - Click **Select Key** to see a list of available keys and choose one to assign.
 - Once assigned, the following data is listed:
 - Key ID
 - Manufacturer

- **PIN**

Note: The PIN requirement is specified on the [Settings](#) screen (**HOTPin|Settings|General|Passcode PIN**).

- ♦ **User will create PIN** – displays if PINs are required; select to allow user to create the PIN either during login or on the HOTPin User Website.

Note: See [HOTPin User Website](#) for important details about end user self-provisioning.

- ♦ **Set PIN** – displays if PINs are required; select to enter and confirm the PIN if you will not allow users to create their own PINs.

Note: While you should indicate that a PIN was assigned on the [HOTPin User Login Information Sheet](#), to maintain security you should convey the PIN value through another means.

The topics in subsequent sections explain user account setup or management tasks.

Change User Account Settings

The Edit User screen includes two tabs:

- General – view/edit user account information.
- Token – view token key information and manage settings.

You can edit properties for [individual users](#) or [groups of users](#). Details are provided in the following sections, grouped by tab.

To edit user properties:

1. Navigate to **HOTPin|Users**.
2. Select one or more users from the list.
3. Click **Properties**.
4. Select the tab you want to edit.
5. Click **OK** save changes and return to the HOTPin screen.

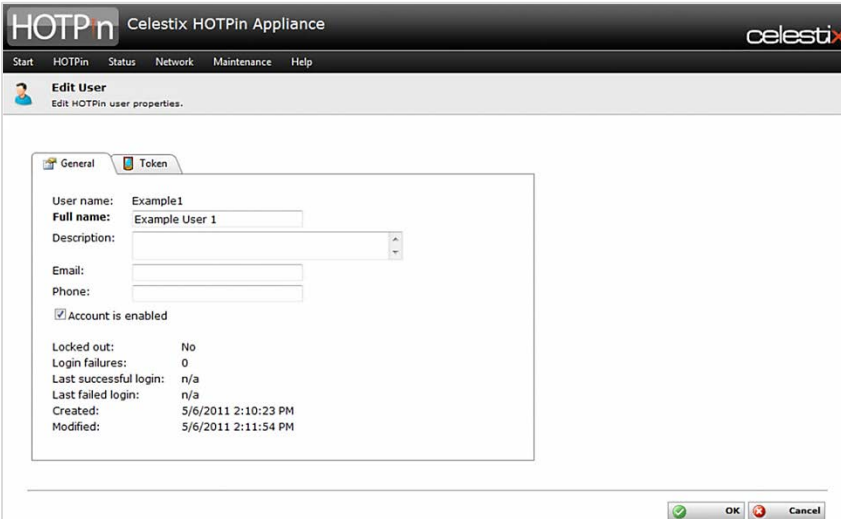
Important: If AD Synchronization is enabled, user email and phone data may be designated for syncing; if so, HOTPin accounts must be noted in the **exclusion list** to maintain changes entered through the web UI.

Edit Individual Users

The following details the settings available for individually selected user accounts on both the General and Token tabs.

General Tab

Illustration 19 provides a reference for the General tab settings described below.



The screenshot shows the 'HOTPin' web interface with the 'Edit User' dialog box open. The 'General' tab is selected, showing fields for 'User name' (Example1), 'Full name' (Example User 1), 'Description' (a dropdown menu), 'Email', and 'Phone'. There is a checkbox for 'Account is enabled' which is checked. Below these fields is a section with login statistics: 'Locked out: No', 'Login failures: 0', 'Last successful login: n/a', and 'Last failed login: n/a'. At the bottom of this section are 'Created: 5/6/2011 2:10:23 PM' and 'Modified: 5/6/2011 2:11:54 PM'. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

Illustration 19 - User Property Settings General Tab

View or edit the following properties for individual users:

- **User name** – displays the HOTPin login name.
- **Full name** – edit the account holder's name.
- **Description** – review/edit optional notes for the user account.

- **Email** – edit the user's standard email or email-to-SMS address. The email address field is optional but may be needed by custom token providers.
- **Phone** – edit the user's mobile phone number. This field is optional but may be needed by custom token providers.
- **Account is enabled** – select to enable user account, deselect to disable user account.

Note: The email-to-SMS messaging function requires a mobile provider service that supports it.

Note: Disabled accounts count towards the user license limit.

Locked out – view account status; this information can help to debug user access issues.

- **Login failures** – view account status; this information can help to debug user access issues.
- **Last successful login** – view account activity for the most recent event granted access; this information can help to debug user access issues.
- **Last failed login** – view account activity for the most recent event denied access; this information can help to debug user access issues.
- **Created** – view the date a user was added to the system.
- **Modified** – view the date that the user record was last changed either by the system or through the **HOTPin|Users|Properties** page.

Token Tab

Illustration 20 provides a reference for the Token tab settings described below.

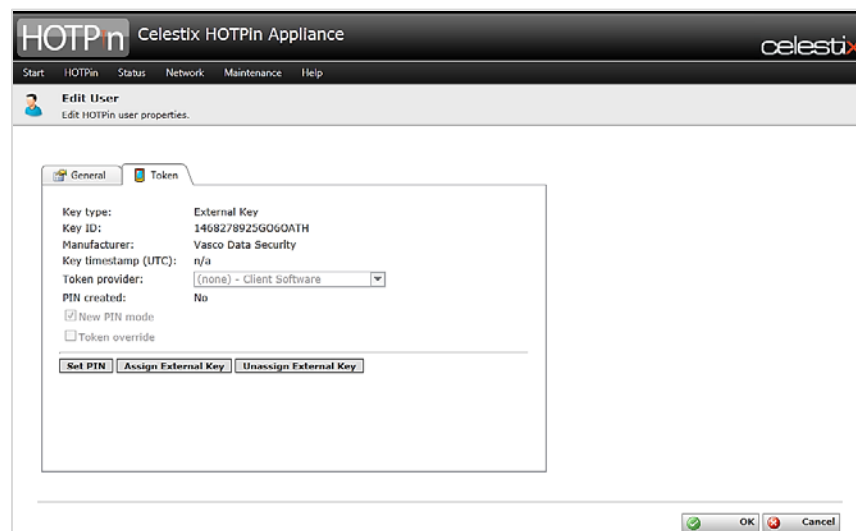


Illustration 20 - User Property Settings Token Tab

View or edit the following individual user properties:

- **Key type** – lists key origin:

- **Internal HOTPin key** for client software or token provider.
 - **External Key** for imported keys (as used in hard token devices).
- **Key ID** – displays the token’s unique ID relative to the user. The key ID is useful when validating that a user has the current token key installed in their client software token application.
- **Key timestamp (UTC)** – displays the token generation detail.
- **Token provider** – edit the assigned token method by selecting an option in the drop list.

Note: If you change the token method from client software to a provider and then back to client software, the user will need to be sure the client has the current key.
- **PIN created** – **Yes** indicates the user account has a PIN; **No** indicates the user will need to create one at the next login if a pin is required.
- **New PIN mode** – select to require a user to create a new PIN, either at the next login or through the HOTPin User Website. A dimmed check box can indicate New PIN Mode has been assigned, or that the PIN requirement has been disabled (see Settings : **PIN**).
- **Token Override** – available when the PIN requirement is invoked; select to allow a user to login with only their PIN and no code. This flag is designed to allow temporary access if the user does not have the device they use for token codes; it can only be set after the user has created a PIN. A dimmed check box indicates either that this feature is unavailable because the PIN requirement has been disabled (see Settings : **PIN**) or that the user is in New Pin Mode.
- **Set PIN** – displays if PINs are required; click to open the Set PIN window where you will enter and confirm the PIN.

Note: See Settings : **Passcode PIN** for PIN requirement information.
- **Assign external key** – click to assign an imported key.

Note: Only administrators can **assign external keys** to user accounts.
- **Unassign external key** – click to remove an imported key and add an internal key to the account.

Edit Groups of Users

When editing properties for a group of users, you will have access to these settings:

Modify just the selected users or all users

- **Selected users** – click to apply changes to the accounts selected on the Users screen.
- **All users** – click to apply changes to all HOTPin accounts.

For each of the options below, you will need to select the edit control checkboxes for the feature settings you want to change; that will enable the property to be selected and/or edited.

General Tab

Illustration 21 provides a reference for the General tab settings described below.

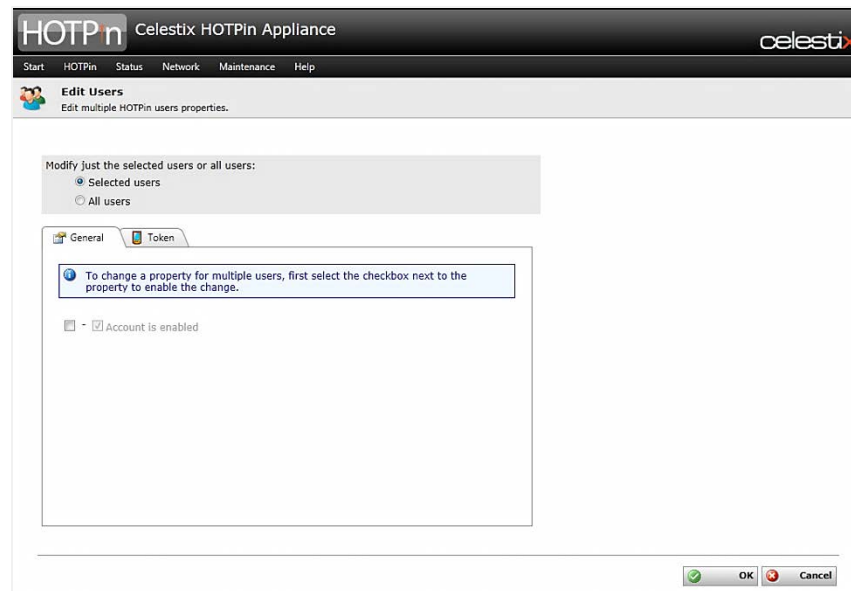


Illustration 21 - Edit Group of Users General Tab

View or edit the following properties for selected users:

- **Account is enabled** – check to activate accounts; uncheck to disable accounts.

Note: Disabled accounts count towards the user license limit.

Token Tab

Illustration 22 provides a reference for the Token tab settings described below.

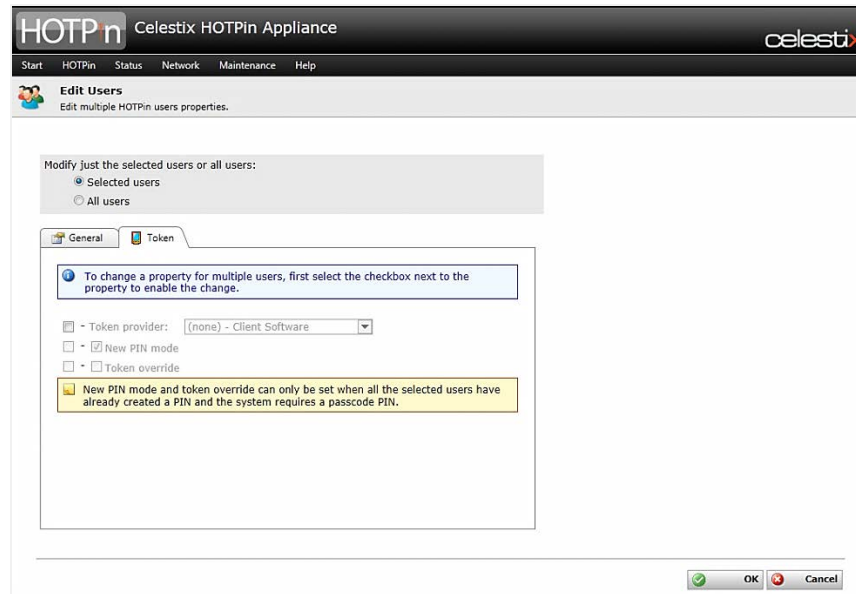


Illustration 22 - Edit Group of User Token Tab

View or edit the following properties for selected users:

Note: If an account that has been assigned an external key is included in the selection, you will not be able to enable editing.

- **Token provider** – edit the assigned token method by selecting an option from the drop list.
- **New PIN mode** – select to require users to create new PINs at the next login. A dimmed check box can indicate that New PIN Mode has already been assigned to at least one user, or that the PIN requirement has been disabled in HOTPin settings (see Settings : [Passcode PIN](#)).
- **Token override** – select to allow a user to login without a token code; the user will just provide a PIN. This flag is designed to allow temporary access if the user does not have the device they use for token codes; it can only be set after the user has created a PIN. A dimmed check box indicates this feature is unavailable because the PIN requirement has been disabled (see Settings : [Passcode PIN](#)) or one of the selected users is in New Pin Mode.

Import Users

Importing user definitions from Active Directory or a plain text file can simplify adding accounts to HOTPin, especially when adding a group of users. The user import wizard allows you to select which users to import to the system and displays an import results page.

To import users:

1. Navigate to **HOTPin|Users**.

2. Click **Import**.
3. On the **Import Users** screen, click **Next**.

The import wizard takes you through the steps to add users to HOTPin. Those steps include:

- **Welcome** – the Welcome screen displays the number of available user licenses.

The menu at the left of the screen indicates your progress in the wizard.

- **Import Source** – select either:

- ♦ Active Directory
- ♦ Text file

The AD option requires credentials to import from the server. The text file option requires you to create a list of users with specific formatting.

- **Source Information**

- ♦ **Active Directory** – the **Import from Active Directory** properties section below provides additional information to help complete this step.
- ♦ **Text file** – the **Import from a Text File** properties section below provides additional information to help complete this step.

- **Select Users** – review the list of accounts created from the import. Deselect any users you do not want to include.

The AD option allows one token provider to be assigned per batch of imports. Options under **Default User Properties**, include:

- ♦ **No change** – leaves a previously assigned method intact if one was designated, or assigns the default method (client software).
- ♦ **(none)**
- ♦ **ClxEmailOtp – Email OTP Provider**
- ♦ **ClxHttpOtp – HTTP OTP Provider**
- ♦ **ClxSmsOtp – SMS OTP Provider**

The text import option includes provider assignment in the formatted data, but you can use the default selector to override the provider assignment for the import group.

Note: Hard tokens must be **assigned** individually to user accounts.

- **Finish** – follow onscreen instructions.

From this screen, you can still return to previous step and make changes.

- **Import Results** – review import summary information.

Click the **Close** button to return to the **Users** screen.

Important: If AD Synchronization is enabled, you will need to add the imported accounts to the **exclusion list** to avoid automatic deletion.

Please Note:

- › You will not be able to add more users than are allowed by your user license.
- › In AD domains, HOTPin user names should be the same as the AD authentication property. See [Active Directory](#) for more information.

As noted above, the subsequent sections provide details for completing user import.

Importing from Active Directory

Illustration 23 provides a reference for the initial AD import screen:



Illustration 23 – Source Information (AD) Screen

Your appliance must be able to access the AD domain controller to pull user accounts. You will need the following for the Source Information screen:

- **Server address/hostname** – enter the AD server information (for example, adserver or 192.168.0.1).
- **User (domain\name)** – enter user account information that has permission to read from Active Directory (format example: ACME\user).
- **Password** – enter the password for the account name entered above.
- **Select by** – choose the option to review available user accounts for import:
 - ♦ **User List** - displays a list of accounts; select check boxes to include user(s) in the import.

- ♦ **Drill Down** – displays a complete list of Active Directory information that can be expanded; select check boxes to include user(s) in the import.
- **Use as a user name if found** – choose an option that will designate an AD property as the HOTPin user name. Options include:
 - ♦ SAM Account Name
 - ♦ Principal Name
 - ♦ Email Address
 - ♦ Domain and SAM Account Name

Notes:

- Once you select an AD authentication property to use as the HOTPin name, you should use the same property as the user name for all HOTPin accounts.
- AD user accounts that do not contain the data in the property selected above will not be included in the list on the Select Users screen.

- **Show disabled users** – check to include inactive AD accounts.

Click the **Search** button to compile a user account selection list in the pane on the right.

Importing from a Text File

You will create a text file (.txt) that contains the user data you want to import. The user information must be comma separated and formatted as follows:

- First line of the file must contain the text:
[Users]
- Each line after defines a user as:
 - ♦ (user name),(full name),(description),(email),(mobile phone),(provider),(enabled)
 - ♦ The first two fields [(user name) and (full name)] are required, but the rest are optional; the additional commas can be left out or the field left blank.

Important: If you include some of the optional data in your text file, you must include data or a comma for all of the optional fields; otherwise some of your data may end up in the wrong field once imported.

- ♦ For the (provider) field, leave blank to assign client software. For a custom provider, use the token provider ID which can be found in the ID column on the **HOTPin|Providers** page.
- ♦ For the (enabled) field, use "0" or "False" for disabled and "1" or "True" for enabled. If the (enabled) field is not provided, it is assumed to be true.

The following examples show the minimum and maximum information to be included in the users file.

Minimum information examples:

```
[Users]
jsmith,John Smith
mjane,Mary Jane
```

Please Note: In the above example, all the users will be added with the default software token and will be active.

Maximum information examples:

```
[Users]
jsmith,John Smith,Remote access user
jsmith.,jsmith@acme.com,1.222.555.1111,,1
mjane,Mary Jane,Remote access user
mjane,2225553333@txt.att.com,1.222.555.3333,CltEmailOtp,1
jlee,Jason Lee,,,,,0
```

Please Note: In the above example, **mjane** was added with a custom token provider, and **jlee** was added with the default provider (note the successive commas used for blank field entries) but set to inactive.

Assign an External Key to a User Account

This section provides details for assigning external keys to user accounts. If your organization uses devices like hard tokens, you will first need to [import token keys](#) for those devices to HOTPin. Then you can assign the keys, and thus the device to user accounts.

Please Note: They are called external keys because HOTPin does not generate them.

To assign an external key:

1. Navigate to **HOTPin|Users**.
2. Select a user from the list.
3. Click **Properties**.
4. Select the **Token** tab.
5. Click **Assign External Key**.
6. Select a key from the **Assign Key** list.

7. Click **OK**.
8. Click **OK** to confirm assignment.
9. Click **OK** save changes and return to the HOTPin screen.

Client Software

Client software token applications, also referred to as client software, are programs that run on different user devices and are used to generate token codes. End users can download their own software if the [HOTPin User Website](#) is enabled. If not, you will need to download the software and provide it to your users. System administrators can download some client software installation files and all client documentation from the web UI. Some applications are only available from the associated download site for the device platform (Android™ and iOS are examples). The download page includes instructions for all client software.

Please Note: To maintain synchronization with the server, a user should only use one token generation method – client software (the default), an external key, or a token provider.

To download client software:

1. Navigate to **HOTPin|Client Software**.
2. Client software and instructions are grouped by device. Use the screen button to toggle between expanded (V) and collapsed (>) views.
3. Select the link for the appropriate software application and follow the on-screen instructions complete the download.
4. Click the **Close** button to return to the HOTPin screen.

Illustration 24 below provides a reference.

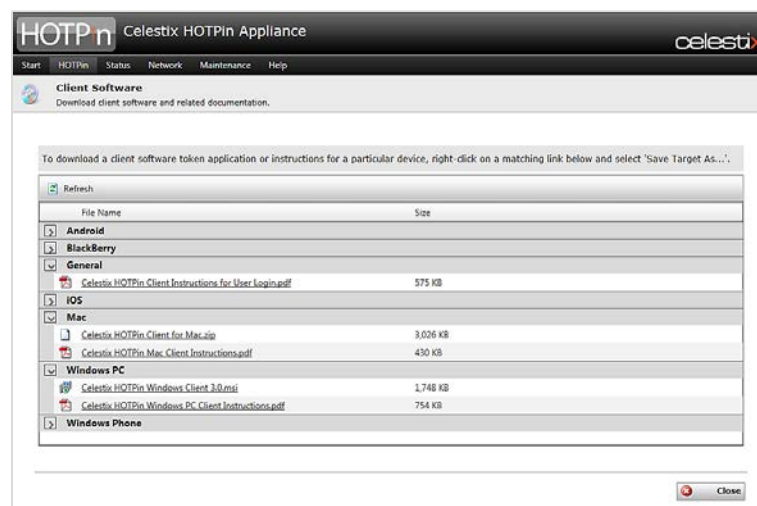


Illustration 24 - Client Software Screen

The install file will download to the local machine.

After downloading and installing the client software on the user device, a token key must be loaded into the client software to generate token codes for network login.

Download User Token Key

Client software needs to be configured with user information that is referred to as token key configuration. The configuration contains a key, data, and settings that are specific to the individual user account. Attaining the key is referred to as downloading a key on the server side, and importing a key on the client side. A key configuration can be imported from either a file location accessible to the user device, a message sent by email or SMS, or from a local area network connection between the client device and the HOTPin User Website.

It can be easier to allow users to download their own key configurations through the HOTPin User Website. However, if a client device cannot access the network, the download feature in the admin site web UI allows you to create a key configuration that you can use or provide for import to the device.

For more information about importing key configuration over a local area network, see [Enable the User Website](#).

Please Note: The key download feature is disabled for accounts that have been assigned an external key.

To download the token key configuration for a user:

1. Navigate to **HOTPin|Users**.
2. Select a user from the list.
3. Click **Download Key**.
4. Select a key configuration option.
See [Key Configuration Formats](#) below for download options.
5. Enter information in the download form.
6. Create the configuration.
7. Click **Cancel** to exit the Download Key page when you are finished downloading the token key.

Key Configuration Formats

The token key configuration comes in three formats, a file, QR code, or data string. The file option can be used with any device that has the ability to import a DAT file. The QR code requires that the device be present and have a camera through which it can scan the code. The string option is intended to be used with devices that have cut and paste functionality, but the string can also be entered manually. The following sections provide instructions for each of the format options.

Please Note: Depending on device capabilities and the client software version, some import formats may not be supported. Check the client software instructions for the version you are using for import functionality.

File

Download property configuration options include:

- **Passphrase** – protect the key configuration with optional encryption. The file passphrase feature provides security while the key configuration is in transit. The passphrase is case sensitive, should be between 6-16 characters, and cannot contain spaces. If entered here, it must also be provided to the user.
- **Require key passphrase** – select to require users to create a passphrase in client software during token key import. Users will then be prompted for the passphrase each time they open HOTPin or when they load the encrypted key. The key passphrase is different from the file passphrase described in the **Passphrase** item above; it can protect the key from being accessed by anyone other than the user who imported it.
- **Clear key file after import** – if possible, force the client software token application to overwrite and/or delete the key configuration file after the key has been imported to the client. This helps to prevent both later reimporting the key (when it would be out of sync with the server application) and access by a malicious program.
 - Note:** Some devices do not support file overwrite functionality by the client application.
- **Download File** – click to save the configuration file locally.

Next, the file will need to be imported to the client software.

See the following [Key Configuration Transfer](#) topic for information about providing the file to end users.

Please Note: The default settings for the **Require key passphrase** and **Clear key file after import** properties are assigned on the HOTPin

Settings page, but administrators can override the default on the [Download Key](#) screen.

QR Code

Download property configuration options include:

- **Passphrase** – to maintain a secure process, you will need to create a passphrase to encrypt the configuration. The passphrase will then be used during import to the client application. The configuration will not be usable without the passphrase. The passphrase is case sensitive, should be between 6-16 characters, and cannot contain spaces.
- **Confirm** – reenter the passphrase.
- **Code size** – select an image size based on the size of the screen you are viewing and the device's field of focus.
- **Require key passphrase on client software** – select to require users to create a passphrase in client software during token key import. Users will then be prompted for the passphrase each time they open HOTPin or when they load the encrypted key. The key passphrase is different from the code passphrase described in the **Passphrase** item above; it can protect the key from being accessed by anyone other than the user who imported it.
- **Generate QR Code** – click to create the image.

Next, the code needs to be scanned into the client application through the device.

String

Property configuration options include:

- **Require key passphrase on client software** – select to require users to create a passphrase; they will then be prompted for the passphrase each time they open HOTPin or when they load the encrypted key. This passphrase can protect the key from being accessed by anyone other than the user who imported it.
- **Space out string** – add blank spaces at regular intervals to make it easier for users who need to manually enter the string in client software.
- **Key configuration string** – copy the string from this field.
- **Create String** – click to generate the key configuration.
- **Copy to Clipboard** – available on Windows systems.

Next, the string will need to be imported to the client software.

See the [Key Configuration Transfer](#) topic below for information about providing the string to end users.

Key Configuration Transfer

After downloading a key configuration, adding it to client software depends on the device capabilities. Potential methods to transfer file or string token key configurations to the user device include:

- Connect directly to the device
- Send through email
- Copy to external media (for example, flash drive, memory card)

The Next Step

You have finished the basic configuration steps for your HOTPin deployment. Your environment or deployment may involve additional features that require configuration that is not part of base-level setup. See [Additional Features](#) for a list.

Next you should save a snapshot of the system image to preserve the initial configuration. After you have an appliance image copy, you should check for software updates that apply to your appliance.

Create a System Image

Once you have set up your appliance and configured the HOTPin application, creating a snapshot will provide an option to help remediate issues that may result from future system updates or changes.

You have two options to access the system image functionality:

- The web UI System Imaging feature (**Maintenance|System Imaging**).
- The front panel display Last Good Version (LGV) feature (access through the Jog Dial).

In each option the image is created in the recovery system process where the main operating system is not running. Thus system can be restored to the initial configuration even if the operating system performance or functionality has been affected. Neither option above is recommended in lieu of a normal backup procedure.

The System Imaging option requires the use of a web browser, but can run when the operating system is loaded (online), or after a restart before the appliance boots into the operating system (offline). Online, or real-time, images use more disk space than offline imaging, but they don't interrupt the services your appliance provides.

The LGV feature is an offline tool and requires that the system be rebooted to access it. But it can be run from the front panel and is convenient if you don't have a monitor and keyboard attached to the appliance.

System Image

Illustration 25 provides a reference for the System Imaging screen.

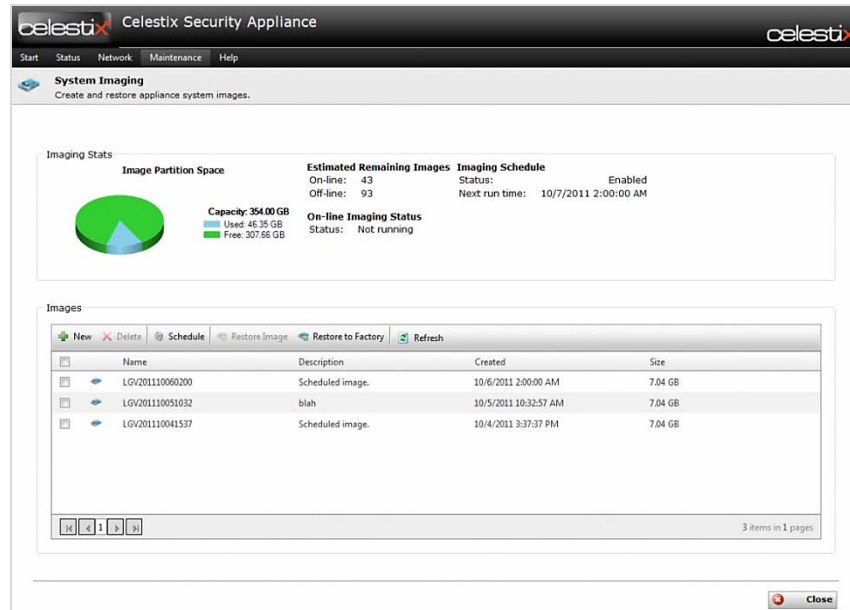


Illustration 25 - System Imaging Screen

To create a system image:

1. Navigate to **Maintenance|System Imaging**.
2. Click **New**.
3. Select the image type:
 - **Online System Image** – the appliance will continue to operate normally while the system image is run, which creates a larger file but doesn't interrupt the services provided by the appliance.
 - **Offline System Image** – the appliance will create the system image while the operating system is offline; this creates a smaller file size but involves a restart that interrupts the services provided by the appliance. See the on-screen note for estimated offline imaging time.
4. Add a **Description** to include relevant information about the image; this can help differentiate from files that were scheduled images.

Note: An image name will be automatically created by appending date/time information to the designation "LGV".
5. Click **OK** to save the image.

Online imaging progress will display on the New Image screen, but you can close and monitor progress on the System Imaging screen as well.

Offline imaging will reboot the appliance to complete, and the web UI will return to the Start screen when the copy process is finished. If the process takes longer than the estimate, the browser may not be able to reconnect to the web UI; refresh your browser by clicking its reload button to continue managing your appliance.

LGV

The LGV instructions below require direct access to the Celestix appliance.

To create an LGV:

Notes:

- You will need to shut down your appliance and then start it again to access the system recovery process.
- It may help to read through all of the instructions before starting the procedure.

1. Shutdown the appliance.
2. The front panel display shows the **System Off** message after shutdown has completed.
3. Press the Jog Dial to start the appliance; the front panel display shows **System On**, and the system beeps for system startup.
4. Next the front panel display shows the **System Ready** message, and the system will beep again. On this second beep, turn the Jog Dial clockwise two full rotations to initiate the recovery system.

Note: Timing when you turn the Jog Dial is more important than how long you turn it. Two full rotations should be adequate to start the recovery system process.

5. The front panel display will show **Celestix Appliance Installer** when the recovery process launches. Menu options will display when the recovery system has loaded.
6. Turn the Jog Dial to scroll to the option **Create Last Good Version <<** and press to select.
7. Confirm the operation when prompted.

The **Saving System Image** screen will show a progress indicator and an estimated time to completion for the image copy process.

After the image has been created, the system will reboot. **DO NOT ACCESS OR TURN OFF THE APPLIANCE DURING THIS PROCESS.**

The appliance will shut down when the LGV process is complete.

Now that you have completed the configuration steps and system image creation, you should check for appliance software updates. See the next section for information.

Update Software

The Software Update Service allows administrators to keep appliance software current through hotfixes, service packs, and upgrades. Software updates include the following applications:

- Windows Server
- Celestix Comet
- Celestix HOTPin

After you have configured your appliance and created an image snapshot, use the Software Update Service to ensure you have the latest application patches for all your appliance software.

Access the update service through the web UI (**Maintenance|Software Updates**). See the online help if you need additional information.

Thank you for purchasing the Celestix HOTPin Appliance. You have now completed all the setup and configuration steps for base-level deployment.

Appendices

Use the links to jump to a topic:

- [HOTPIn Glossary](#)
- [Web User Interface Content Overview](#)
- [Additional Features](#)
- [API Extensions](#)
- [Safety Precautions](#)
- [Product Reclamation and Recycling](#)
- [Network Information Worksheet Form](#)

HOTPin Glossary

Note: Links in **bold** type navigate out of the Glossary.

Active Directory group

Groups can be designated in the AD Synchronization feature to automatically add, edit, or delete HOTPin user accounts.

Active Directory organizational unit

OUs can be designated in the AD Synchronization feature to automatically add, edit, or delete HOTPin user accounts.

AD Synchronization

Manage HOTPin user accounts automatically by linking the user database to AD. Also referred to as syncing.

authentication failure counter

A feature that tracks the number of unsuccessful login attempts. Administrators set a maximum number of authentication failures (see **Configure System Settings**), and a user account exceeding that number is locked out from system access.

backup server

The backup server is part of the HOTPin **High Availability** feature. The backup server pulls configuration information from a primary HOTPin server to provide authentication service redundancy.

client software

An application that runs on a user device to generate the token codes required for user authentication. The HOTPin Client is a client software token application. It is abbreviated in the documentation as client software, and may also be referred to as a soft token.

client software token application

The descriptive name of the client software. It is abbreviated in the documentation as **client software**.

custom provider

See **token provider**.

custom token provider

See [token provider](#).

default software token

The client software token application is the default software token in the HOTPin system.

exclusion list

The exclusion list is an [AD Synchronization](#) feature that severs the link between the HOTPin user database and AD for individually specified accounts.

event log

The HOTPin event log records HOTPin system management and user authentication events.

exclusion list

The exclusion list is an [AD Synchronization](#) feature that severs the link between the HOTPin user database and AD for individually specified accounts.

external key

An external key is used by hard tokens to generate token codes.

full name

The first and last name as entered in the user account.

group

See [Active Directory group](#).

HA

See [high availability](#).

hard token device

A hard token is a device, like a key fob, for example, that generates token codes. It uses an external key that must be imported HOTPin; it can be used in lieu of client software or a token provider.

high availability

Array deployment option for redundancy/failover.

HOTP

HMAC-Based (Hashed Message Authentication Code) One-Time Password Algorithm (RFC 4226).

HOTPin

HOTPin is a system that provides two-factor authentication services for Celestix appliances. HOTPin normally uses a PIN and token code to create a passcode. You can also configure HOTPin for one-factor authentication using just the token code for authentication. The system includes a server application, client software token applications (client software) and token provider options.

HOTPin User Website

When enabled, the user provisioning site allows end users to setup HOTPin accounts, token generation method, and client software.

increment authentication failures

A security feature that limits the number of times a user is sent a token code before successful authentication. When enabled, the user's login failure counter is incremented each time a provider sends a token code, and the user will be locked out if they exceed the maximum limit as defined in the [Maximum Authentication Failures](#) setting.

internal key

An internal key is used in client software to generate token codes.

key configuration

See [token key configuration file](#).

log files

Log files contain the HOTPin system's archived events or data.

login page

The web page a user will access to enter network system/HOTPin credentials. Also referred to as a portal page.

maximum authentication failures

The limit of unsuccessful login attempts before a user is locked out from system access. Access this feature on the [Settings](#) page.

network access server

A component of [RADIUS](#) authentication. Abbreviated NAS.

Network Policy Server

See [NPS](#).

new pin mode

The feature that requires a user to create a PIN at their next login attempt when PINs are required (see [Settings](#)). This setting allows a user to log in one time with just a valid token code.

Next Code

The name of the screen button in client software applications that users click to generate a token code.

NPS

NPS, or Network Policy Server, is how Microsoft implements RADIUS. The NPS RADIUS feature allows you to configure RADIUS clients. It also provides access to the Windows NPS management application.

NPS RADIUS

See [NPS](#).

one-time password

One-time passwords (OTPs) combine with PINs to create passcodes when PINs are required. When PINs are not required, OTPs serve as the user passcode. Client software token applications generate OTPs, or the HOTPin server can send OTPs through a token provider. OTPs are also referred to as [token codes](#).

Organizational Unit (OU)

See [Active Directory group](#).

OTP

One-time password; also referred to as a [token code](#).

OTP look ahead value

The setting that establishes a window of valid token codes available for authentication (Settings|General|Authentication).

passcode

In two-factor authentication, the passcode is the combination of a user's [PIN](#) and a [one-time password \(token code\)](#). In single-factor authentication, the token code serves as the passcode.

passphrase

A security feature that encrypts the token key used by HOTPin client software. A passphrase has two possible functions: it can encrypt the token key configuration file or it can be required by a system administrator to force a user to encrypt access to the token once imported to client software.

PIN

A user-defined Personal Identification Number that is combined with a [one-time password \(token code\)](#) to create a [passcode](#). The PIN requirement is an optional setting that is configured on HOTPin's [Settings](#) page.

portal page

The web page a user will access to enter network system/HOTPin credentials. Also referred to as the login page.

primary server

The primary server is part of the HOTPin High Availability feature. The primary server provides authentication services under normal operating conditions. It is queried by a backup server for data so that the backup server can provide authentication services if the primary is unavailable.

provider

See [token provider](#).

provider send command string

A feature of custom token providers, the send command string is a value assigned by the system administrator that lets users request a token code from the HOTPin system. The command string is not case sensitive and can contain a maximum of 7 characters. Access this feature on the [Settings](#) page.

RADIUS

Remote Access Dial In User Service (RADIUS) is an authentication protocol ([RFC 2865](#)). The HOTPin system uses the Microsoft application Network Policy Server (NPS) to implement RADIUS.

RADIUS client

A RADIUS client is a network access server (NAS) that facilitates authentication requests between access clients and the HOTPin system when RADIUS is used as the authentication protocol.

Remote Access Dial In User Service

See [RADIUS](#).

send command string

See [provider send command string](#).

sent code TTL

The value that limits the number of minutes a token code sent by a custom provider is valid. Access this feature on the [Settings](#) page.

sent token code

A [token code](#) that has been sent by email or SMS to a user from the HOTPin system. Token codes are synonymous with one-time passwords (OTPs).

Settings

The HOTPin server application web user interface page where administrators can access Authentication, Token Provider, and Client Software settings.

shared secret

RADIUS components (clients, proxies, and servers) use a password verify and encrypt communication they share.

software token

A software application that runs as a client on PCs or mobile devices to generate token codes for use in both single and two-factor authentication; also referred to as **client software**.

software token application

See **software token**.

standalone server

The standalone server is used when only one HOTPin server is deployed; it is the default setting in the HOTPin **High Availability** feature.

sync

Sync may refer to:

- **AD Synchronization**
- The status of external components (like client software or hard tokens) with relation to server components (like token keys)

token code

Token codes are also referred to as one-time passwords (OTPs); they combine with **PINs** to create **passcodes** when PINS are required. When PINs are not required, token codes serve as the user password/passcode. Client software token applications generate token codes, or the HOTPin server can send token codes through a token provider.

token device

See **hard token device**.

token generation counter

User accounts use a token generation counter to keep client software and token providers synchronized with the server application. The synchronization process allows for a window of valid token codes to facilitate authentication.

token key

The HOTPin component that contains a user's encryption configuration information. Client software must have a token key to generate valid token codes. Users must have a distinct key for each HOTPin system they access.

token key configuration

When a key is used in a token it includes some user data and other information like a counter and passphrase requirements. The additional information composes the token key configuration.

token key configuration file

The file created when a user's token key is downloaded. The file includes the user's token key, counter, and passphrase requirements. The configuration file can be downloaded by a system administrator and provided to a user through email or removable media, or, if the [HOTPin User Website](#) is enabled, the user can download it.

token provider

A feature that sends token codes to users through the HOTPin system. Custom providers are used as alternatives to installing and running client software on a user device to generate a token code. For example, token codes can be sent through email or email-to-SMS.

UAG trunk

A repository of published applications for user access; often accessed through a portal page. Applies to deployments with a WSA appliance.

user

Person with access rights to a network system. Users have two states:
Active – user will be able to authenticate in the login process.
Inactive – user will fail to authenticate in the login process.

user device

A PC or mobile device used to generate or receive [token codes](#) to be used in [passcodes](#). Some user devices may be also be used to access a network system.

user name

A login name that uniquely identifies a user. A user name should be between 4 and 128 characters long and cannot include spaces.

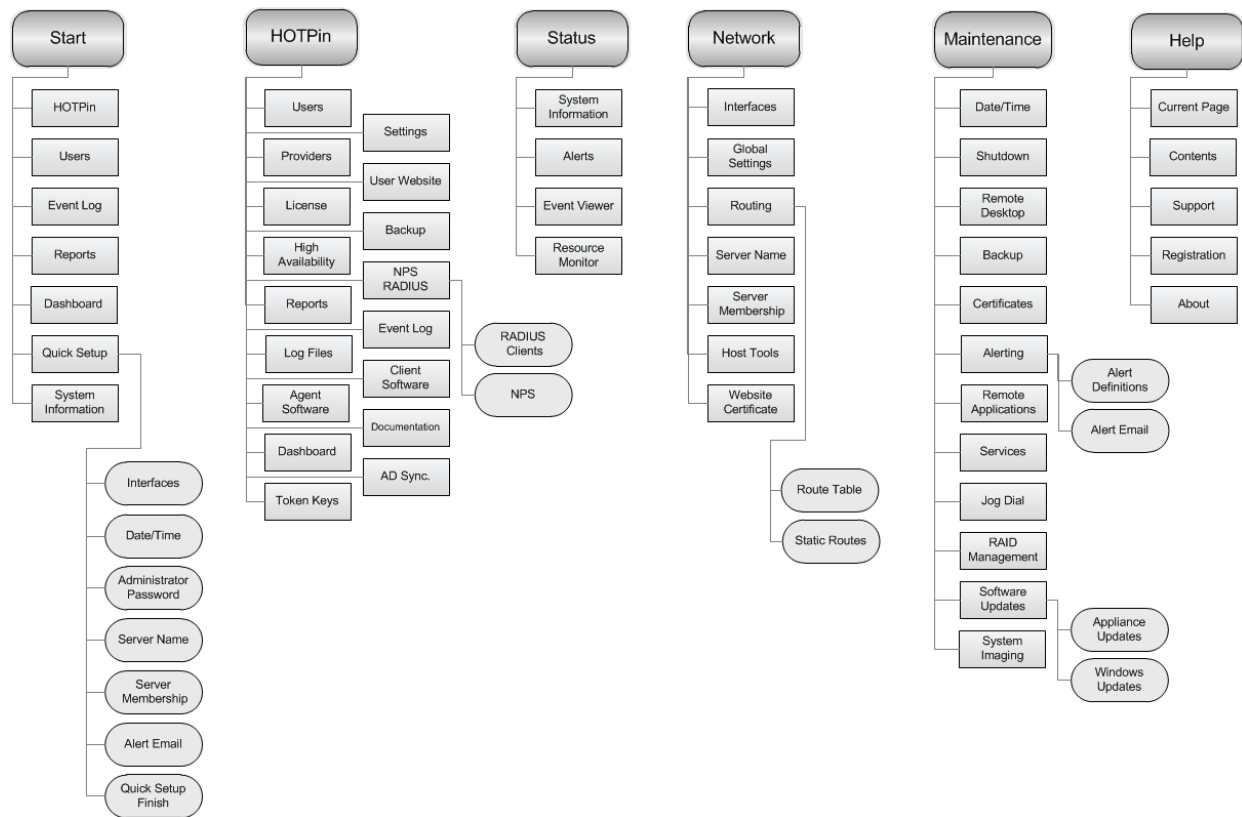
user token codes

See [token code](#).

Web User Interface Content Overview

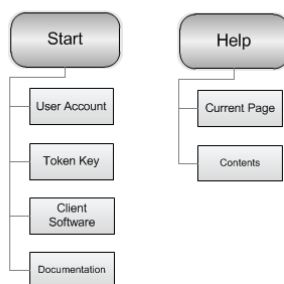
The web UI menu structure is outlined below. Use it to quickly find the feature you need.

HOTPin Appliance Web User Interface Menu Diagram



The HOTPin User Website structure is outlined below.

HOTPin User Website Menu Diagram



Additional Features

For information about configuring the following features, see the HOTPin online help.

- **High Availability** – deploys a primary and backup server for redundancy.
- **NPS RADIUS** – allows HOTPin to use Microsoft's Network Policy Server to provide RADIUS authentication services.
- **Agent Software** – configure the HOTPin appliance for a UAG environment.

API Extensions

The following features have sample code libraries in the HOTPin SDK.

- Agent 1.1 – extends agent functionality to allow authentication to any website login page.
- Authentication API for .NET/Java – creates an authentication communication channel for ASP .NET and Java-based websites and applications.
- QR Code Authentication for .Net/Java – allows authentication through a web page using client software.

Contact your sales representative for more information:

sales@celestix.com

Safety Precautions

- Do not overload the AC supply branch circuit that provides power to the server.
- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded electrical outlet that is easily accessible at all times.
- Unplug the power cord from the inlet on the appliance rear panel to disconnect power to the server.
- Do not place anything on the power cords or cables. Arrange them so that no one can accidentally step on or trip over them. Do not pull on a cord or cable. When unplugging the cord from the electrical outlet, grasp the cord by the plug.
- Do not plug telecommunications/telephone connectors into the NIC connectors.
- This server contains an internal lithium battery. There is a risk of fire and burns if battery is not handled properly. Do not attempt to recharge the battery. Do not expose the battery to temperatures higher than 60 °C. Do not disassemble, crush, puncture, short external contact, or dispose of battery in fire or water.
- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by Celestix. Dispose of used batteries according to local regulations for hazardous waste.

WARNING:

- ! RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
- ! DISPOSE OF USED BATTERIES ACCORDING TO HAZARDOUS WASTE PROCEDURES AS REQUIRED IN YOUR AREA.
- ! HAZARDOUS MOVING PARTS.
- ! KEEP FINGERS AND OTHER BODY PARTS AWAY.

Product Reclamation and Recycling

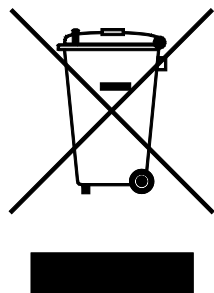
Celestix Networks is committed to environmentally responsible behavior. As part of this commitment, we work to comply with environmental standards such as the European Union's Waste Electrical and Electronic Equipment (WEEE) Directive and the Restriction of Hazardous Substances (RoHS) Directive.

These directives and other similar regulations from countries outside the European Union regulate electronic waste management and the reduction or elimination of specific hazardous materials in electronic products. The WEEE Directive requires electrical and electronics manufacturers to provide mechanisms for the recycling and reuse of their products. The RoHS Directive restricts the use of certain substances that are commonly found in electronic products today. Restricted substances include heavy metals, like lead and polybrominated materials. The RoHS Directive, with some exemptions, applies to all electrical and electronic equipment.

In accordance with Article 11(2) of Directive 2002/96/EC (WEEE), products put on the market after 13 August 2005 are marked with the following symbol or include it in their documentation: a crossed-out wheeled waste bin with a bar beneath.

Celestix Networks provides recycling support for our equipment to comply with the WEEE Directive. For recycling information, send e-mail to recycling@celestix.com indicating the type of Celestix Networks equipment that you wish to dispose of and the country where it is currently located, or contact your Celestix Networks account representative.

Products returned through our reclamation process are recycled, recovered, or disposed of in a responsible manner.



Network Information Worksheet Form		
Property	Network Information	
Computer Name		_____
Administrator Password	[Celest1x] (default – change during setup)	_____
Workgroup or Domain name		_____
Network Adapters (LAN0)	IP Address: _____ Subnet Mask: _____ Default Gateway: _____ Primary/Secondary DNS Server: _____ _____ Static Routes: _____ Network Address: _____ Gateway Address: _____	_____ _____ _____ _____ _____ _____ _____
Network Adapters (LAN1)	IP Address: _____ Subnet Mask: _____ Default Gateway: _____ Primary/Secondary DNS Servers: _____ Primary/Secondary WINS Servers: _____	_____ _____ _____ _____ _____
Network Adapters (LAN2 +)	Include the IP Address/Subnet Mask for each adapter you will use:	_____ _____ _____ _____ _____ _____
Active Directory Server	IP Address: _____ Hostname: _____	_____ _____
Application Server (if applicable)	IP Address: _____ Hostname: _____	_____ _____